No. 2024-1365

United States Court of Appeals for the Federal Circuit

CPC PATENT TECHNOLOGIES PTY, LTD.,
Appellant

v.

APPLE, INC.,
Appellee

Appeal from the United States Patent and Trademark Office,
Patent Trial and Appeal Board in No. IPR2022-00600

BRIEF OF APPELLANT CPC PATENT TECHNOLOGIES PTY, LTD.

K&L GATES LLP

GEORGE C. SUMMERFIELD
JONAH B. HEEMSTRA
70 W. Madison Street, Suite 3300
Chicago, IL 60602
(312) 372-1121
george.summerfield@klgates.com

DARLENE F. GHAVIMI-ALAGHA
2801 Via Fortuna, Suite 650
Austin, Texas 78746
(512) 482-6800

Attorneys for Appellant

April 29, 2024

CHALLENGED CLAIMS

[1pre] A method of enrolling in a biometric card pointer system, the method comprising the steps of:

[1a] receiving card information;

[1b] receiving the biometric signature;

[1c] defining, dependent upon the received card information, a memory location in a local memory external to the card;

[1d] determining if the defined memory location is unoccupied; and

[1e] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

[2pre] A method of obtaining verified access to a process, the method comprising the steps of:

[2a] storing a biometric signature according to the enrolment method of claim 1;

[2b] subsequently presenting card information and a biometric signature; and

[2c] verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

[19pre] A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

[19a] code for receiving card information;

[19b] code for receiving the biometric signature;

[19c] code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

[19d] code for determining if the defined memory location is unoccupied; and

[19e] code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

[20pre] A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

[20a] code for storing a biometric signature according to the enrolment method of claim 19;

[20b] code for subsequently presenting card information and a biometric signature; and

[20c] code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CERTIFICATE OF INTEREST

Case Number 24-1365

Short Case Caption CPC Patent Technologies Pty Ltd. v. Apple Inc.

Filing Party/Entity CPC Patent Technologies Pty Ltd.

Instructions:

1. Complete each section of the form and select none or N/A if appropriate.
2. Please enter only one item per box; attach additional pages as needed, and check the box to indicate such pages are attached.
3. In answering Sections 2 and 3, be specific as to which represented entities the answers apply; lack of specificity may result in non-compliance.
4. Please do not duplicate entries within Section 5.
5. Counsel must file an amended Certificate of Interest within seven days after any information on this form changes. Fed. Cir. R. 47.4(c).

I certify the following information and any attached sheets are accurate and complete to the best of my knowledge.

Date: 04/29/2024

Signature: /s/ George Summerfield

Name: George Summerfield

1. Represented Entities. Fed. Cir. R. 47.4(a)(1).	**2. Real Party in Interest.** Fed. Cir. R. 47.4(a)(2).	**3. Parent Corporations and Stockholders.** Fed. Cir. R. 47.4(a)(3).
Provide the full names of all entities represented by undersigned counsel in this case.	Provide the full names of all real parties in interest for the entities. Do not list the real parties if they are the same as the entities. ☑ None/Not Applicable	Provide the full names of all parent corporations for the entities and all publicly held companies that own 10% or more stock in the entities. ☐ None/Not Applicable
CPC Patent Technologies Pty Ltd.		Charter Pacific Corporation Limited

☐ Additional pages attached

4. Legal Representatives. List all law firms, partners, and associates that (a) appeared for the entities in the originating court or agency or (b) are expected to appear in this court for the entities. Do not include those who have already entered an appearance in this court. Fed. Cir. R. 47.4(a)(4).

☐ None/Not Applicable ☐ Additional pages attached

Brian P. Bozzo (K&L Gates LLP)		

5. Related Cases. Other than the originating case(s) for this case, are there related or prior cases that meet the criteria under Fed. Cir. R. 47.5(a)?

☑ Yes (file separate notice; see below) ☐ No ☐ N/A (amicus/movant)

If yes, concurrently file a separate Notice of Related Case Information that complies with Fed. Cir. R. 47.5(b). **Please do not duplicate information.** This separate Notice must only be filed with the first Certificate of Interest or, subsequently, if information changes during the pendency of the appeal. Fed. Cir. R. 47.5(b).

6. Organizational Victims and Bankruptcy Cases. Provide any information required under Fed. R. App. P. 26.1(b) (organizational victims in criminal cases) and 26.1(c) (bankruptcy case debtors and trustees). Fed. Cir. R. 47.4(a)(6).

☑ None/Not Applicable ☐ Additional pages attached

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5, counsel for Appellant states that: (a) no other appeal in or from the same proceeding was previously before this or any other appellate court, whether under the same or a similar title; and (b) the following cases will be directly impacted by this court's decision in the pending appeal:

ASSA ABLOY AB, et al. v. CPC Patent Technologies PTY, LTD., IPR2022-01094 (PTAB);

ASSA ABLOY AB, et al. v. CPC Patent Technologies PTY, LTD., IPR2022-01093 (PTAB);

ASSA ABLOY AB, et al. v. CPC Patent Technologies PTY, LTD., No. 3:22-cv-00694 (D. Conn.);

CPC Patent Technologies PTY, LTD. v. HID Global Corporation, No. 6:22-cv-01170 (W.D. Tex.); and

CPC Patent Technologies PTY, LTD v. Apple Inc., No. 5:22-cv-02553 (N.D. Cal.).

Consolidated Appeal Nos. 24-1492, -1493 are directed to IPR proceedings IPR2022-01093 and -01094, respectively. Those appeals are proceeding concurrently to the instant case.

JURISDICTIONAL STATEMENT

On September 18, 2023, the Board issued a final written decision ("FWD") determining claims 1, 2, 19, and 20 to be invalid. CPC timely requested director review on November 3, 2023, which was denied on November 21, 2023. CPC timely appealed on December 18, 2023. This Court therefore has jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. § 141(c).

INTRODUCTION

United States Patent No. 8,620,039 (the "'039 Patent") is directed to a method and system to "efficiently and securely permit a user to store biometric information during an enrollment process." Appx5. The claims at issue on appeal involve a discrete method of steps that involves, (1) receiving card information and a biometric signature, (2) defining, dependent upon the received card information, a memory location in a local memory external to the card, (3) determining if the defined memory location is unoccupied, and (4) if the defined memory location is unoccupied, storing the biometric signature at the defined memory location. Appx77, cl. 1; Appx79, cl. 19.

Despite the clear and unambiguous series of steps in the Challenged Claims, the PTAB relied on a hodge podge of prior art references, ranging from casino gaming machines to grocery store rewards accounts, to erroneously find Claims 1, 2, 19, and 20 (the "Challenged Claims") unpatentable. The Board construed the term "defining" to mean "set[ting]" or "establish[ing]," and then relied on art that merely ***identifies*** a ***previously*** set or established memory location to find the prior art rendered obvious the "defining" limitation. Appx36, Appx39. Thus, under even the Board's construction, the prior art does not render obvious the Challenged Claims, and its finding otherwise was clearly erroneous. The Court should reverse the Board's final written decision and uphold the validity of the Challenged Claims.

STATEMENT OF THE ISSUE

1. Whether the PTAB erred in finding the Challenged Claims of the '039 Patent unpatentable as obvious in the absence of substantial evidence in the identified art for the limitation "defining, dependent upon the received card information, a memory location in a local memory external to the card."

STATEMENT OF THE CASE

A. The '039 Patent

The '039 Patent issued on December 31, 2013, from an application claiming priority of August 12, 2005. Appx64. As the PTAB noted, the '039 Patent "describes a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during an enrollment process, and in future verification processes access their account using an identification (ID) card and biometric information such as a fingerprint." Appx5.

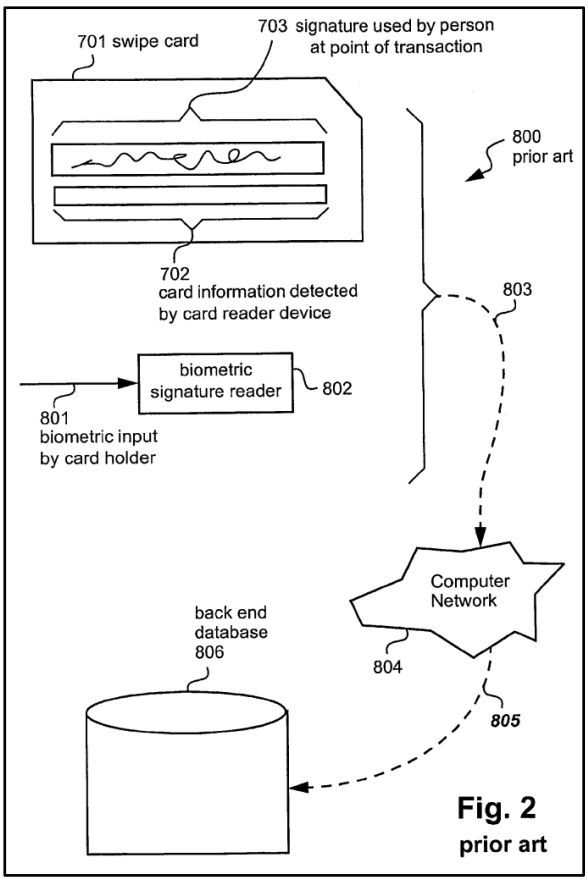
The invention of the '039 Patent is designed to solve for prior art arrangements with a "cumbersome" central repository of card information and biometric information, which "potentially compromises the privacy of the holder of the card," and which "requires complex back-end database management," as well as a "complex and expensive" "front-end biometric signature reader" with "storage and/or processing capabilities." Appx72, 2:10-22.

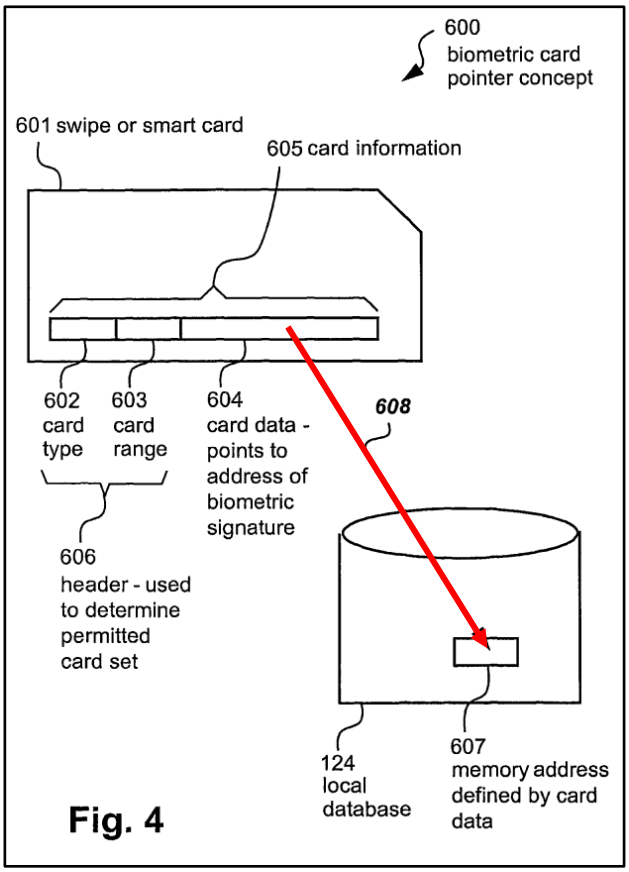
"The '039 patent explains that in the enrollment phase '[t]he card user's biometric signature is automatically stored . . . at a memory address ***defined by the ('unique') card information on the user's card*** as read by the card reader of the verification station.'" Appx3 (quoting Appx72, 2:62-67) (emphasis added). Representative claim 1 of the '039 Patent reads as follows:

> A method of enrolling in a biometric card pointer system, the method comprising the steps of receiving card information;
>
> receiving the biometric signature:
>
> defining, dependent upon the received card information, a memory location in a local memory external to the card;
>
> determining if the defined memory location is unoccupied; and
>
> storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Appx77, 12:29-38.

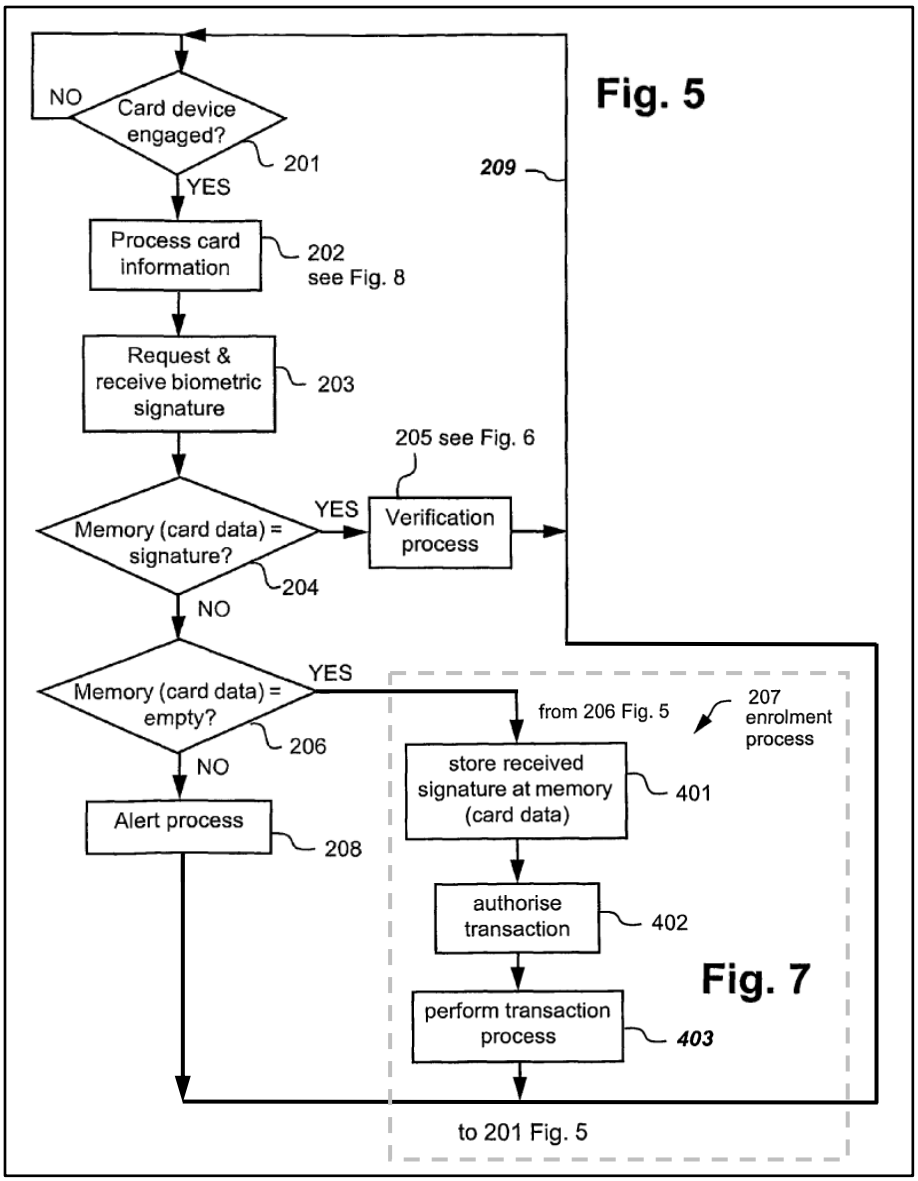
The contrast between the prior art and the patented invention is depicted in Figures 2 and 4:





Appx66, Fig. 2; Appx68, Fig. 4 (annotated).

As shown in Figure 4, "the card data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an address 607 in the local database 124." Appx75, 7:31-34. The claimed information flow during an enrollment process is graphically depicted in Figures 5 and 7 of the '039 Patent:



Appx69-70, Fig. 5, Fig. 7.

As is clear from these figures and the accompanying text, card information is processed first (step 202), a biometric signature is received next (step 203), and the enrollment process occurs thereafter, using a memory location that has been identified as being "empty" (steps 206 and 207). Appx75, 8:22-60; *see also* Appx3-Appx4. From there, in step 401 of Figure 7, the biometric signature received in step

203 is stored in memory 124 at a memory address defined by card data 604 received in step 202 of Figure 5. Appx76, 9:62-67.

The PTAB confirmed that, in the Challenged Claims, "during an enrollment process, the claimed 'biometric signature,' *e.g.*, a fingerprint, is not yet stored in the memory and no memory location or address has been 'set' or 'established' for the fingerprint."[1] Appx30; *see also* Appx36 ("Overall, in terms of 'defining' . . . we understand that during an enrollment process, the claimed 'biometric signature,' *e.g.*, a fingerprint, is not yet stored in the memory, and no memory location or address has been 'defined,' as in 'set' or 'established,' in the memory for storing the fingerprint, until card information is received").

B. The Prior Art

Apple urged a single challenge ground – obviousness under section 103(a) in light of Bradford, Foss and Yamane. Appx8; Appx94. As will be demonstrated herein, that combination fails to teach "defining, dependent upon the received card information, a memory location in a local memory external to the card," as required by the subject claims.[2]

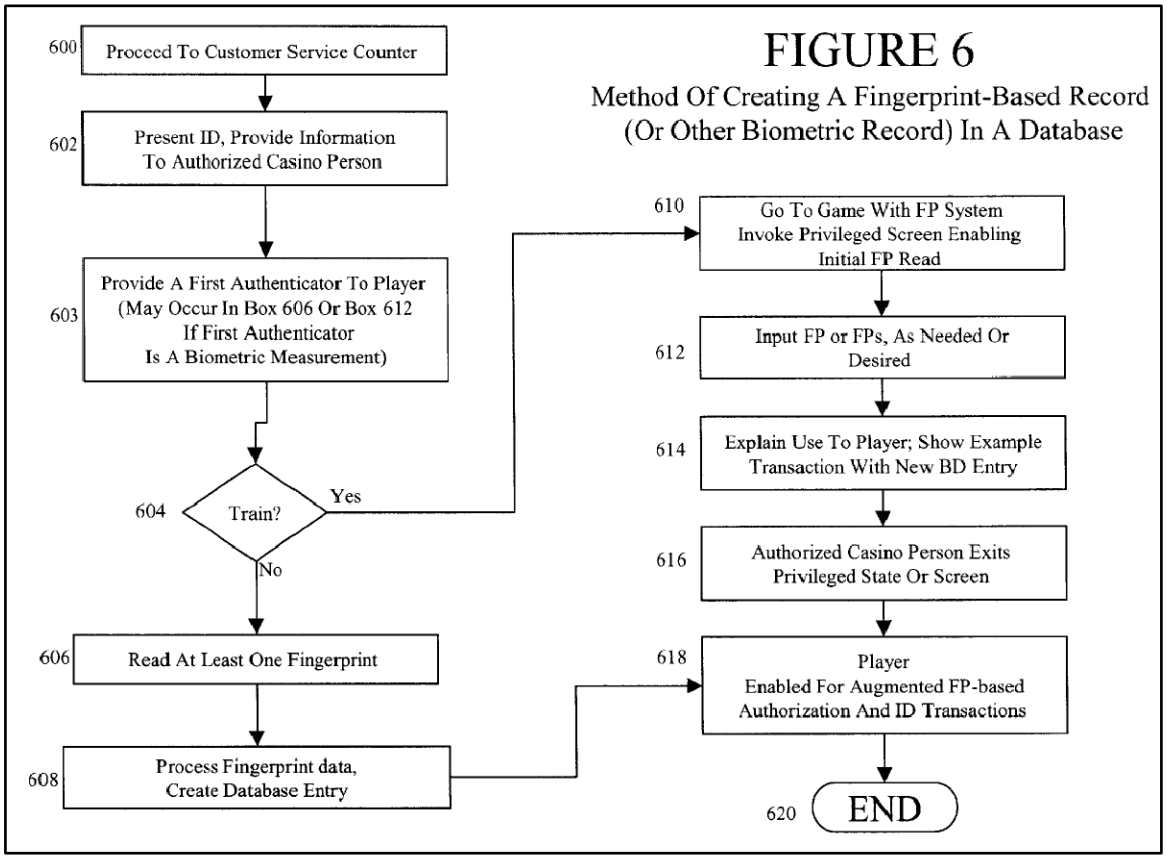
---

[1] The PTAB construed "defining" in the Challenged Claims to mean "sets" or "establishes." Appx36, Appx39.

[2] For purposes of this Appeal, only the Bradford and Foss references are relevant.

1. Bradford

As the PTAB notes, "Bradford discloses a gaming authentication system that uses at least two authenticators to identify a player, explaining '[t]he first authenticator may be one of many types, with a typical first authenticator being a player ID card, a voucher with a unique, encoded, and preferably encrypted numerical ID on it, a unique alphanumeric sequence, or an RFID tag,'" while "[t]he second authenticator will be based on a biometric reading." Appx14. The following depicts the steps described in Bradford:



Appx1012, Fig. 6.

As Bradford explains with regard to this figure, "[a] player currently without an entry in the player ID database would first go to a customer service counter and ask for an account, box 600," whereupon "[t]he process then moves to box 602, where an authorized person ***enters the initial data from the player into the database***." Appx1029, 14:21-27 (emphasis added). At step 606, the user enters the "biometric measurement." Appx1030, 16:26-31. At step 608, "the system creates the entry in the player ID database corresponding to this player, ***associating the data corresponding to a first and second authentic authenticator with this entry***." *Id.*, 16:40-43 (emphasis added).

Nothing in Bradford teaches defining a memory location dependent upon card information as required by the Challenged Claims. In fact, by Apple's own characterization, Bradford teaches using "first authenticator" data from a card to locate ***already-stored*** biometric information:

> Bradford teaches the first authenticator data read from the card ***points to*** the second authenticator data ***stored*** in the player entry in the player ID database (Appx112 (emphasis added));
>
> The first authenticator data read from the card is used as a reference ***to locate*** a player entry having a matching first authenticator data (*id.* (emphasis added));
>
> Because the first authenticator data in the player entry is associated with the second authenticator data, the first authenticator data is used '***to get***' the corresponding second authenticator data (*id.* (emphasis added));
>
> Bradford teaches a method for authenticating electronic funds transfers, where the system requests the player's first authenticator. The first

> authenticator is typically a player ID 'of some kind, including but not limited to a traditional player ID card, a voucher ID.' The system then determines if the presented first authenticator (e.g., player ID) 'correspond[s] to at least one entry ***in the player ID database***' (Appx113 (emphasis added) (internal citations omitted)); and
>
> A POSITA would have understood information ***pointing to*** one entry in the player ID database is information pointing to a particular memory location at an address in the player ID database or that such is obvious (Appx114 (emphasis added)).

The PTAB also recognized that Apple's expert, Dr. Sears, "testif[ied] that Bradford teaches a process in which the steps are ***reversed*** - a memory location is defined before any card information is received." Appx45 (emphasis added).

2. Foss

Foss "describes various systems and methods for transferring funds between stored value card accounts of first and second customers." Appx16. Figure 8 of Foss depicts "an enrollment process at merchant terminal 704 for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program." *See id.*

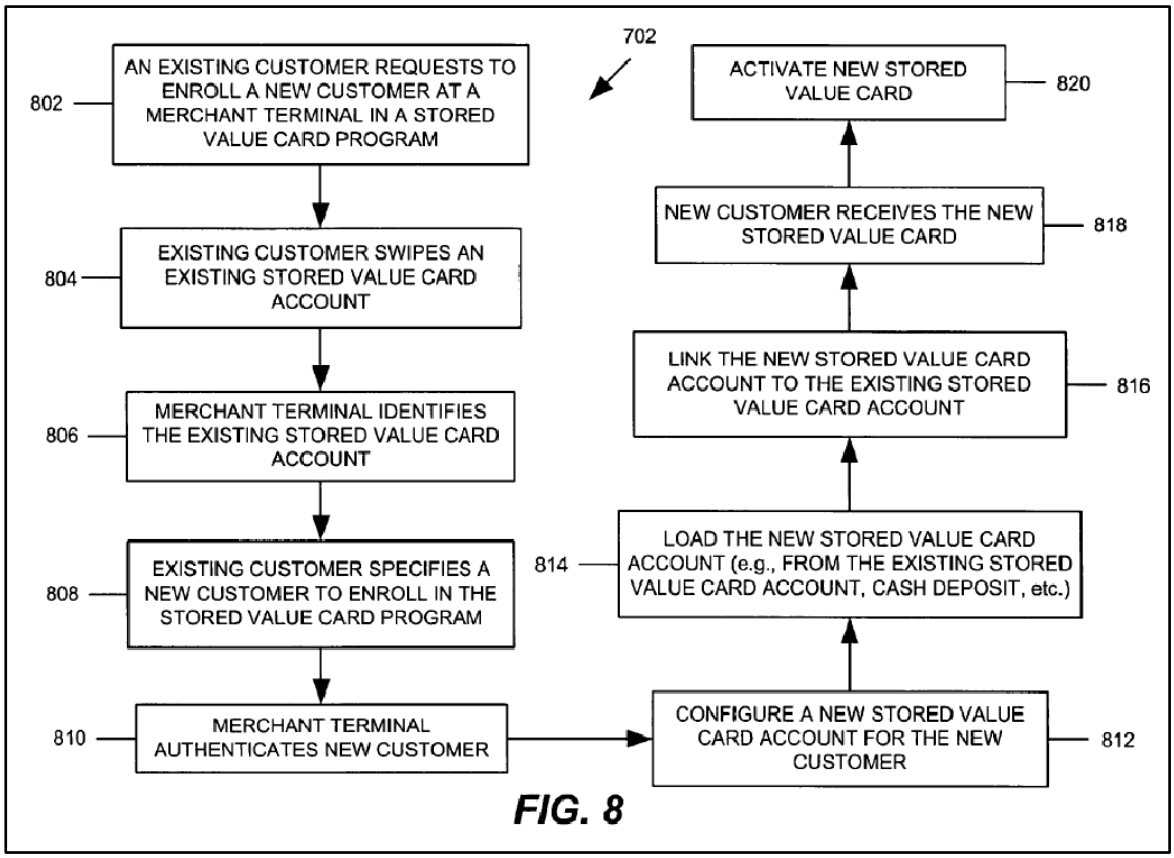


FIG. 8

Id.; Appx1056, Fig. 8.

In Foss, an ***existing*** customer, with an existing account, swipes a card to begin an enrollment process for new ***additional*** customers, and the new customer's account is added to the existing customer's account. Appx17. A new stored value card is linked to the existing stored value card account. *Id.*

As Apple recognized, Foss "discloses a method for enrollment of user information that looks up ***an existing record*** using card information." Appx96 (emphasis added); *see also* Appx117 ("in this embodiment, ***an account already exists***, and the customer is 'initiat[ing] an enrollment process'" (emphasis added)). Thus, the record in Foss is already "stored in the memory," and the memory location

thereof "has been 'set' or 'established"' ***prior to*** enrolling a new customer, meaning Foss does not teach defining a memory location "dependent upon the received card information," as required by the Challenged Claims. *See* Appx30 (in the Challenged Claims, "during an enrollment process, the claimed 'biometric signature,' *e.g.*, a fingerprint, is not yet stored in the memory and no memory location or address has been 'set' or 'established' for the fingerprint").

C. Procedural Background

Apple petitioned for review of the '039 Patent on a single obviousness challenge ground involving the two afore-discussed references in addition to Yamane. Appx40; Appx94.[3] As noted above, the PTAB recognized that Apple's "expert, Dr. Sears, 'testif[ied] that Bradford teaches a process in which the steps are ***reversed*** - a memory location is defined before any card information is received.'" Appx45 (*quoting* Appx319 (emphasis added)). The PTAB did not take issue with Patent Owner's characterization of Dr. Sears' testimony on this point. Rather, it stated that such testimony does not conflict with claim 1, "as the creation of a player account . . . prior to receiving the card information does not preclude subsequently identifying a memory location . . . and establishing that memory location as the

[3] Yamane was not used in connection with the "defining" limitation and is thus not relevant to this Appeal. Appx106; *see also* Appx23-25.

location where new biometric data, *e.g.*, a player's fingerprint, is going to be stored." *Id*.

This brought the PTAB to Foss, which purportedly "teaches how, i.e., using card data to define, that is—to establish or set a memory location, e.g., the player's user account, for storage of the biometric information in a local memory." Appx46. Petitioner's characterization of Foss, however, contradicts the Board's finding. The following, in fact, was the entirety of the Petition's substantive discussion regarding the Foss reference in the context of the "defining" limitation:

> *Foss* teaches a system and method for transferring funds between stored value card accounts. *Foss* teaches 'an enrollment process…for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program.' Thus, in this embodiment, an account already exists, and the customer is 'initiat[ing] an enrollment process.' To initiate enrollment, the customer is prompted 'to swipe the ***existing*** stored value card' to '***continue*** the ***enrollment*** process.' The system 'identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706.' Thus, *Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card.

Appx116-117 (emphasis in original) (internal citations omitted).

The PTAB additionally professed confusion over what it described as CPC's "moving target" construction of "defining." Appx33. The example purportedly underlying that confusion actually relates to ***creating*** a player ID entry rather than ***defining*** a memory location:

> Patent Owner argues that ['defining'] is something more than 'pointing to' or 'finding,' and perhaps means 'creating.' *See* [Appx255] (Patent Owner arguing that 'Bradford, notably, does not teach utilizing the first authenticator to create a player ID entry').

Appx33.

Ultimately, the PTAB found that "Bradford discloses an enrollment process including receiving card information and biometric information, but does not describe specifically *how* to store the biometric information, [and that] Foss teaches how, i.e., using card data to define, that is—to establish or set a memory location, e.g., the player's user account, for storage of the biometric information in a local memory." Appx46 (emphasis in original). The PTAB thus concluded that all the Challenged Claims were unpatentable in light of the cited prior art. Appx62.

SUMMARY OF ARGUMENT

The Challenged Claims of the '039 Patent require "defining, dependent upon the received card information, a memory location in a local memory external to the card." The PTAB construed that limitation as precluding a biometric signature (*e.g.*, a fingerprint) already stored in memory, and precluding a memory location or address for the fingerprint already set or established prior to the enrollment process.

In the sole prior art reference combination urged by Apple, the memory location at which fingerprint data is stored during the enrollment process is ***not*** defined by card information received during that process and is instead set or established in advance of receiving a biometric signature such as a fingerprint. As

such, in light of the PTAB's claim construction, as well as the intrinsic evidence underlying that construction, the prior art combination is antithetical to the Challenged Claims, and the PTAB's determination that such combination rendered the Challenged Claims obvious was not grounded in the substantial evidence before the Board.

ARGUMENT

I. STANDARD OF REVIEW

This Court reviews the PTAB's factual findings for substantial evidence and its legal determinations *de novo*. *See, e.g., In re Van Os*, 844 F.3d 1359, 1360 (Fed. Cir. 2017). Obviousness, the sole basis for rejecting the proposed claims below, is a question of law based on subsidiary findings of fact. *Id.* The PTAB "must make findings of relevant facts, and present its reasoning in sufficient detail that the court may conduct meaningful review of the agency action." *In re Lee*, 277 F.3d 1338, 1346 (Fed. Cir. 2002).

II. THE BOARD ERRED IN FINDING THE CHALLENGED CLAIMS OBVIOUS OVER THE PRIOR ART

The single issue raised in this appeal is whether the PTAB erred in finding the Challenged Claims of the '039 Patent obvious in the absence of substantial evidence in the cited art supporting disclosure of the limitation, "defining, dependent upon the received card information, a memory location in a local memory external to the card." As the PTAB noted, a patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103(a); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "[W]hen a patent claims a structure already known in the prior art that is

altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416 (*citing United States v. Adams*, 383 U.S. 39, 50-51 (1966)).

The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). In this case, the Court need analyze only whether the prior art combination cited by Apple actually arrives at the claimed invention. The answer is no, and the PTAB erred in finding the Challenged Claims obvious in light of the prior art cited by Apple.

The single challenge ground before the PTAB was that claims 1, 2, 19 and 20 of the '039 Patent are purportedly obvious over Bradford in view of Foss, and in further view of Yamane. *See, e.g.*, Appx94. In the claimed method: 1) card information is processed; 2) a biometric signature is received; 3) an enrollment process begins using a memory location defined by the card data that has been identified as "empty;" and 4) the biometric signature received is stored in the defined, empty memory location. *See* Appx69, Fig. 5, Appx70, Fig. 7, Appx75, 8:22-60, Appx76, 9:62-67. Apple's expert, Dr. Sears, agreed that this is the claimed order:

> Q: So, again, just to repeat my question it's obtain card information, first; define the memory location based on that information, second; store the biometric signature at that defined memory location, third. That is the order that things happen in Claim 1, right?
>
> A: I believe that is the order in which things need to happen.

Appx1995, lines 2-10.

The PTAB agreed with that claimed order as well, noting that, in the Challenged Claims, "during an enrollment process, the claimed 'biometric signature,' *e.g.*, a fingerprint, is not yet stored in the memory and no memory location or address has been 'set' or 'established' for the fingerprint."[4] Appx30; *see also* Appx36.

Thus, in order to render obvious the Challenged Claims, the prior art combination upon which Apple relies must teach or render obvious such steps performed in that order. *See Hytera Commc'ns Co. v. Motorola Sols.*, 841 Fed. App'x 210, 215-16 (Fed. Cir. 2021) (quoting *Lincoln Nat'l Life Ins. Co. v. Transamerica Life Ins. Co.*, 609 F.3d 1364, 1370 (Fed. Cir. 2010)). In Bradford, however, the primary reference upon which Apple relies, "the steps are ***reversed*** - a memory location is defined before any card information is received." *See* Appx45

[4] The PTAB construed "defining" in the Challenged Claims to mean "sets" or "establishes." Appx36; Appx39.

(emphasis added). As Apple's expert testified, in Bradford, the database entry is created ***first***, *i.e.*, before the first authenticator (player ID card) is created:

> Q: If the first authenticator [in Bradford] is a player ID card that's generated by the casino, ***the database entry is created first***, and the first authenticator is ***then*** created and provided to the user; is that right?
>
> A: I believe from the reading of that one about -- that sounds accurate.

Appx2012, lines 12-18 (emphasis added).

The PTAB did not take issue with Patent Owner's characterization of Dr. Sears' testimony on this point. Appx45 (*quoting* Appx319). Rather, it stated that such testimony does not conflict with claim 1, "as the creation of a player account . . . prior to receiving the card information does not preclude subsequently identifying a memory location . . . and establishing that memory location as the location where new biometric data, *e.g.*, a player's fingerprint, is going to be stored." *Id*. Ultimately, however, the PTAB found that "Bradford discloses an enrollment process including receiving card information and biometric information, but does not describe specifically *how* to store the biometric information . . . ." Appx46 (emphasis in original).

This express deficiency in Bradford brought the PTAB to Foss, which purportedly "teaches how, i.e., using card data to define, that is—to establish or set a memory location, e.g., the player's user account, for storage of the biometric information in a local memory." *See id.* However, Foss does not teach using card

data to define—that is to establish or set—a memory location and determine if the defined memory location is unoccupied, as evidenced by Petitioner's own characterization of the reference in its Petition. The following is the entirety of the Petition's substantive discussion regarding the Foss reference in the context of the "defining" limitation:

> *Foss* teaches a system and method for transferring funds between stored value card accounts. *Foss* teaches 'an enrollment process…for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program.' Thus, in this embodiment, an account already exists, and the customer is 'initiat[ing] an enrollment process.' To initiate enrollment, the customer is prompted 'to swipe the ***existing*** stored value card' to '***continue*** the ***enrollment*** process.' The system 'identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706.' Thus, *Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card.

Appx116-117 (emphasis in original) (internal citations omitted).

CPC addressed this discussion before the PTAB, noting "[t]he portions of Foss quoted [in the Petition] describe 'enabling a primary account holder (*i.e.* ***an existing customer*** 610) to enroll additional new customer(s) in the family stored value program' and that initiating enrollment required the existing customer 'to swipe the existing stored value card' in order to 'continue the enrollment process' for 'additional new customer(s).'" Appx256 (*citing* Appx1075, ¶¶ [0085], [0086], [0088] (emphasis in original) and Appx1055-1056, Figs. 7-8). As Patent Owner

explained, the details in Foss relied upon by the Petitioner "relate[] to the family card, i.e., ***adding additional users to an existing family card account as described above***." Appx255 (*citing* Appx1075, ¶ [0088] (emphasis added); Appx1058, Fig. 10).

Put differently, Foss teaches the memory location was defined, set, and established by the existing family card account. The memory location of the new user was not defined dependent upon received card information as claimed, but was instead defined based on the existing account. Further, because the memory location was defined by an ***existing*** account, the defined memory location was necessarily already occupied by the existing account information.

The PTAB thus relied upon a teaching from Foss where one can add new user information to a memory location ***already defined and occupied*** by data pertaining to an existing user. This runs counter to the PTAB's construction of the Challenged Claims, wherein a fingerprint is not yet stored in the memory, nor is a memory location for such fingerprint defined, "until card information is received." *See* Appx30, Appx36. Admittedly, Foss may teach using a card to ***identify*** a memory location where existing information is already stored in order to store additional information there (the "family stored value program"). Appx1075, ¶ [0088] ("At block 806, merchant terminal 704 identifies the stored value card account associated with the existing customer 610."). It clearly does not teach, however, using a card

to "define," "set," or "establish" the memory location where such additional information is to be stored because that location was already defined, set, and established by the existing customer account information. Appx257; *see also* Appx30, Appx36, Appx39.

Should the construction of "defining" in the Challenged Claims somehow have morphed to include simply identifying where data is already stored, that construction would be inconsistent with that portion of the claim calling for storing the biometric signature at the "defined location" only "if the memory location is ***unoccupied***." Appx77, 12:15-18 (emphasis added). Construing "defining" to include "identifying a memory location of existing information" would also be inconsistent with the PTAB's claim construction, and the opinion of Apple's expert as to the order of claimed method steps. Appx39 (agreeing with CPC that based on "the proper interpretation of 'defining,' … 'the biometric information isn't stored yet.'"); Appx1995, lines 2-10.

Finally, on the issue of claim construction, the PTAB professed confusion over what it described as Patent Owner's "moving target" construction of "defining." Appx33. The Board cited CPC's argument that Bradford "does not teach utilizing the first authenticator ***to create a player ID entry***." *Id.* (emphasis added) (citing Appx255). Obviously, CPC's example pertains to ***creating*** a player identification entry to be stored in a memory location, rather than ***defining*** the memory location

in which that entry is to be stored once created. *See* Appx254-255. Any confusion is solely attributable to the mismatch between the PTAB's own construction of "defining" and the teachings of the Bradford-Foss reference combination. In short, that combination does not teach the claimed "defining, dependent upon the received card information, a memory location in a local memory external to the card," and the PTAB's conclusion finding this limitation taught by the prior art is unsupported by substantial evidence. As Apple did not propose further modifying that combination to reverse the order of process steps resulting from such combination, there is no issue to address on remand, and the PTAB's decision should be reversed.

CONCLUSION

For the foregoing reasons, the PTAB's decision that the Challenged Claims of the '039 Patent are obvious should be reversed.

Dated: April 29, 2024

Respectfully submitted,

By: /s/ George C. Summerfield

GEORGE C. SUMMERFIELD
george.summerfield@klgates.com
JONAH B. HEEMSTRA
jonah.heemstra@klgates.com
K&L GATES LLP
70 West Madison Street
Chicago, Illinois 60602-4207
(312) 372-1121

DARLENE F. GHAVIMI-ALAGHA
darlene.ghavimi@klgates.com
K&L GATES LLP
2801 Via Fortuna, Suite 650
Austin, Texas 78746
(512) 482-6800

ATTORNEYS FOR APPELLANT
CPC PATENT TECHNOLOGIES PTY, LTD.

ADDENDUM

INDEX TO ADDENDUM

Trials@uspto.gov
571-272-7822

Paper 22
Date: October 13, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD,
Patent Owner.

IPR2022-00600
Patent 8,620,039 B2

Before SCOTT A. DANIELS, AMBER L. HAGY and FREDERICK C. LANEY, *Administrative Patent Judges.*

DANIELS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Apple Inc., ("Apple" or "Petitioner") filed a Petition requesting *inter partes* review ("IPR") of claims 1, 2, 19, and 20 of U.S. Patent No. 8,620,039 B2 (Ex. 1001, "the '039 patent"). Paper 1 ("Pet"). CPC Patent Technologies PTY, Ltd., ("CPC" or "Patent Owner") filed a Preliminary Response to the Petition. Paper 7 ("Prelim. Resp.").

On October 17, 2022, we instituted trial for claims 1, 2, 19, and 20 of the '039 patent on all grounds of unpatentability alleged in the Petition. Paper 8 ("Decision to Institute" or "Inst. Dec."). After institution of trial, Patent Owner filed a Patent Owner Response. Paper 12 ("PO Resp.). Petitioner timely filed a Reply. Paper 13 ("Pet. Reply). Subsequently, Patent Owner filed a Sur-Reply to address certain arguments raised in Petitioner's Reply. Paper 15 ("PO Sur-Reply).

A hearing for this proceeding was held on July 18, 2023. The transcript of the hearing has been entered into the record. Paper 21 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a).

For the reasons that follow, we determine that Petitioner has met its burden of showing by a preponderance of the evidence that claims 1, 2, 19, and 20 are unpatentable.

A. Real Parties in Interest

Petitioner states that Apple Inc. is the real party in interest. Pet. 57. Patent Owner states that CPC Patent Technologies PTY, Ltd., is the real party in interest. Paper 3.

B. Related Matters

The parties indicate that the '039 patent has been asserted against Petitioner in *CPC Patent Technologies PTY Ltd. v. Apple Inc.*, Case No.

6:21-cv-00165, in the U.S. District Court for the Western District of Texas. Pet. 57; Paper 3.

Petitioner indicates that it has filed additional petitions for *inter partes* review challenging two other patents held by Patent Owner, IPR2022-00601 for U.S. Patent No. 9,269,208, and IPR2022-00602 for U.S. Patent No. 9,665,705. Pet. 57. Final Written Decisions in these IPRs were entered on September 27, 2023.

C. The '039 Patent (Ex. 1001)

The '039 patent, titled "Card Device Security Using Biometrics," describes a biometric card pointer (BCP) system intended to more efficiently and securely permit a user to store biometric information during an enrollment process, and in future verification processes access their account using an identification (ID) card and biometric information such as a fingerprint. Ex. 1001, 2:51–3:11.

The '039 patent explains that in the enrollment phase "[t]he card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase)." *Id.* at 2:62–64. The '039 patent explains further that "[t]he biometric signature is stored at a memory address defined by the ('unique') card information on the user's card as read by the card reader of the verification station." *Id.* at 2:64–67. Following the enrollment phase, the '039 patent describes that

> [a]ll future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby

> determining if the person submitting the card is authorised to do so.

Id. at 3:4–11.[1] For both enrollment and future verification, the use of the ID card at a verification station "is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature ([e.g.] thumb print or retinal scan etc.) to the biometric reader." *Id.* at 3:12–15.

Figure 4 of the '039 patent is reproduced below.

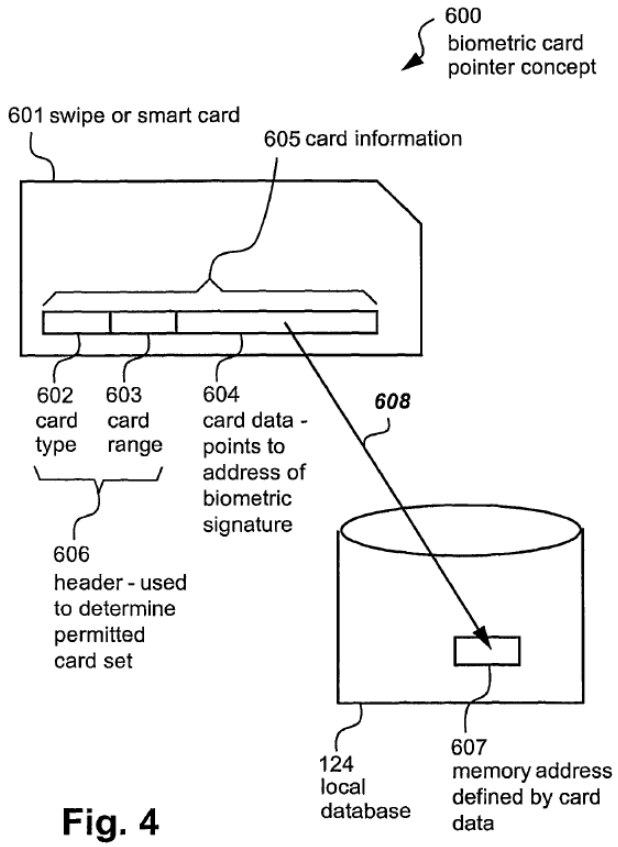


Fig. 4

[1] The words "enrolment," "authorise," and "authorisation" are the British spellings of "enrollment," "authorize," and "authorization." *See, e.g.*, https://www.merriam-webster.com/dictionary/authorisation, last visited Sept. 23, 2022. We will use the American spelling of these words except when quoted from the '039 patent.

Figure 4 of the '039 patent illustrates swipe or smart card 601 including card information 605 encompassing fields for card type 602, card range 603, and card data 604. The '039 patent describes that "the card data 604 acts as the memory reference which points, as depicted by an arrow 608, to a particular memory location at an address 607 in the local database 124." *Id.* at 7:31–35. Information 605 can be encoded on a magnetic strip on the card, for example. *Id.* at 7:28–29. The '039 patent explains that for a specific user "[i]n an initial enrolment phase, . . . [t]he card data 604 defines the location 607 in the memory 124 where their unique biometric signature is stored." *Id.* at 7:43–49. And the '039 patent explains further that "in later verification phases, . . . [t]his signature is compared to the signature stored at the memory location 607 in the memory 124, the memory location 607 being defined by the card data 604 read from their card 601 by the card reader 112." *Id.* at 7:50–56.

Figures 6 and 7, reproduced below, depict the differences between enrollment process 207 shown in Figure 7 and verification process 205 shown in Figure 6.

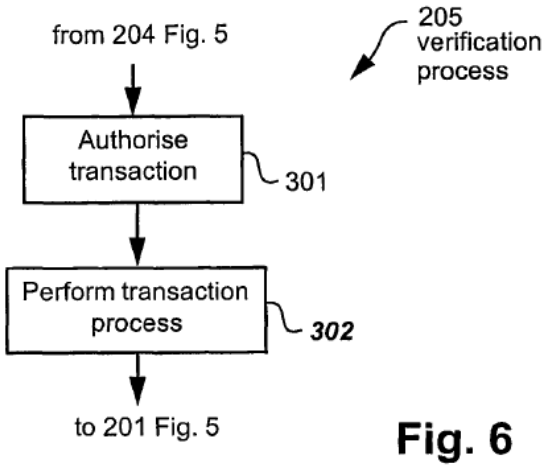


Fig. 6

Figure 6 illustrates verification process 205, which occurs after the enrollment process, illustrated, below, in Figure 7.

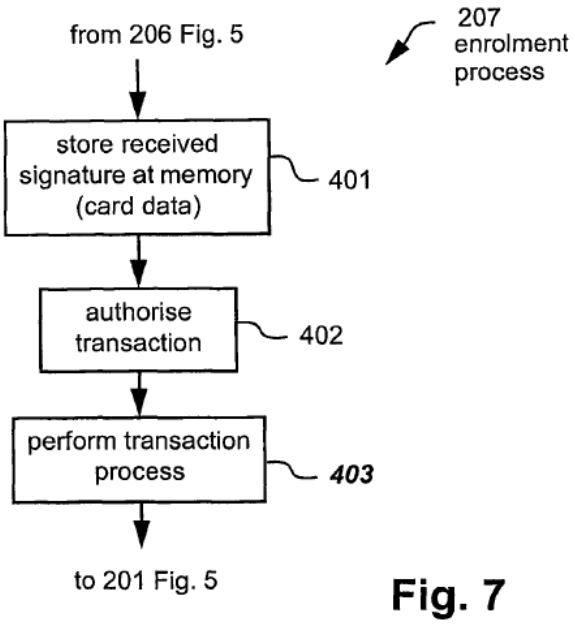


Fig. 7

Figure 7 of the '039 patent illustrates enrollment process 207 where the system at "step 401 stores the biometric signature received by the step 203 in the memory 124 at a memory address defined by the card data 604." *Id.* at 9:64–66 (referring to elements 203 and 124 described in Figure 5).

A difference between verification process 205 and enrollment process 207 is that the enrollment process includes step 401, which *stores* the biometric signature "at a memory address defined by the card data 604," whereas in verification process 205 "step 204 *reads* the contents stored at a single memory address defined by the card data 604" and compares the stored biometric signature with the input biometric signature. *Id.* at 9:65–66, 8:24–26.

D. Illustrative Claim

Claims 1 and 19 are independent. Each of claims 2 and 20 depends, respectively, from independent claims 1 and 19. Claim 1, including disputed

limitations highlighted in italics, illustrates the claimed subject matter and is reproduced below:

> 1. [1Pre] A method of enrolling in a biometric card pointer system, the method comprising the steps of:
>
> [1a] receiving card information;
>
> [1b] receiving the biometric signature;
>
> [1c] *defining, dependent upon the received card information, a memory location in a local memory external to the card;*
>
> [1d] determining if the defined memory location is unoccupied; and
>
> [1e] storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Ex. 1001, 12:29–38. Limitations [1a]–[1e] are similarly recited in independent claim 19 in the context of "a processor to execute a method of enrolling in a biometric card pointer system." *Id.* at 15:25–16:11. For example, limitation [19a] recites "code for receiving card information." *Id.* at 16:3.

E. Prior Art and Asserted Ground

Petitioner asserts that claims 1, 2, 19, and 20 would have been unpatentable based on the following ground:

Ground	Claim(s) Challenged	35 U.S.C. §[2]	Reference(s)/Basis
1	1, 2, 19, 20	103(a)	Bradford,[3] Foss,[4] and Yamane[5]

Petitioner relies on the testimony of Andrew Sears, Ph.D. Ex. 1003. Patent Owner relies on the testimony of William Easttom, Ph.D. Ex. 2001.

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. 35 U.S.C. § 103(a); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). "[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416 (citing *United States v. Adams*, 383 U.S. 39, 50–51 (1966)). The question of obviousness is resolved based on underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence,

[2] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.
[3] Ex. 1004, US Patent No. 6,612,928 Bl (Sept. 2, 2003).
[4] Ex. 1005, US Pub. Appl. No. 2005/0127169 A1 (pub. Jun. 16, 2005).
[5] Ex. 1006, US Pub. Appl. No. 2001/0014883 A1 (pub. Aug. 16, 2001).

objective evidence of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).[6]

The Supreme Court made clear that we apply "an expansive and flexible approach" to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. To support this conclusion, however, it is not enough to show merely that the prior art includes separate references covering each separate limitation in a challenged claim. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness additionally requires that a person of ordinary skill at the time of the invention "would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention." *Id.*

Accordingly, an obviousness determination generally requires a finding "that a person of ordinary skill in the art would have been motivated to combine or modify the teachings in the prior art and would have had a reasonable expectation of success in doing so." *Univ. of Strathclyde v. Clear-Vu Lighting LLC*, 17 F.4th 155, 160 (Fed. Cir. 2021) (citing *OSI Pharms.*, 939 F.3d at 1382 (quoting *Regents of Univ. of Cal. v. Broad Inst., Inc.*, 903 F.3d 1286, 1291 (Fed. Cir. 2018))). "Whether the prior art discloses a claim limitation, whether a skilled artisan would have been motivated to modify or combine teachings in the prior art, and whether she would have had a reasonable expectation of success in doing so are

[6] The parties do not present evidence or arguments regarding secondary considerations.

questions of fact." *Strathclyde*, 17 F.4th at 160. In determining whether there would have been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason why a person of skill in the art would have made the combination. *Metalcraft of Mayville, Inc. v. The Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017). Moreover, in determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103(a) is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985) ("It is elementary that the claimed invention must be considered as a whole in deciding the question of obviousness."); *see also Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983) ("[T]he question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious. Consideration of differences, like each of the findings set forth in *Graham*, is but an aid in reaching the ultimate determination of whether the claimed invention *as a whole* would have been obvious.").

As a factfinder, we also must be aware "of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning." *KSR*, 550 U.S. at 421. Applying these general principles, we consider the evidence and arguments of the parties.

B. Level of Ordinary Skill in the Art

The level of skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). "This reference point prevents . . . factfinders from using their own insight or, worse yet, hindsight, to gauge obviousness."

Id. Moreover, "the inquiry into whether any 'differences' between the invention and the prior art would have rendered the invention obvious to a skilled artisan necessarily depends on such artisan's knowledge." *Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1337 (Fed. Cir. 2020) (citing *Dow Jones & Co. v. Ablaise Ltd.*, 606 F.3d 1338, 1349, 1353 (Fed. Cir. 2010) (affirming the district court's grant of summary judgment of invalidity in part because the obviousness "analysis requires an assessment of the '. . . background knowledge possessed by a person having ordinary skill in the art'")).

Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. *Env't Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. Ltd, Inc. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007).

In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima*, 261 F.3d at 1355.

Additionally, the Supreme Court informs us that "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421.

In our Institution Decision we determined, in accordance with Petitioner's proposal, that a person of ordinary skill in the art at the time of the '039 patent

> would have had at least a bachelor's degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year of experience in the field of human-machine interfaces and device access security. Additional education or experience might substitute for the above requirements.

Inst. Dec. 9 (quoting Pet. 4). Patent Owner does not dispute the level of ordinary skill in the art. PO Resp. 5.

Because there is no express dispute as to the level of ordinary skill in the art, and because Petitioner's assessment is consistent with the '039 patent and the asserted prior art, we maintain our reliance on Petitioner's proposed level of ordinary skill in the art as set forth above.

C. Claim Construction

We construe claims using the principles set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–17 (Fed. Cir. 2005) (en banc), and related cases. 37 C.F.R. § 42.100(b) (2021). Under that precedent, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning the term would have to a person of ordinary skill at the time of the invention, in the context of the entire patent including the specification. *Phillips*, 415 F.3d at 1312–13.

1. Dependent upon

Petitioner indicates that the parties agreed in the district court litigation that "dependent upon," recited in claim 1 and 19, should be given its "[p]lain and ordinary meaning, defined as 'contingent on or determined by.'" Pet. 6 (citing Ex. 1032, 2). Patent Owner agrees, adding that "a

memory location in a local memory which *corresponds* to, but is not contingent upon or determined by, the received card information is not 'dependent upon' under Apple's claim construction." PO Resp. 7 (emphasis added). Patent Owner contends, however, that despite this agreed upon meaning, the arguments in the Petition are not consistent with the plain and ordinary meaning. *Id.*

For purposes of understanding claim 1, given the plain and ordinary meaning of "dependent upon," limitation 1[c] would read:

> [1c] *defining, [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;*

Because neither party disputes the agreed upon meaning of "dependent upon," we will consistently apply the plain and ordinary meaning of "dependent upon" as "contingent on or determined by."

2. Biometric card pointer system

Petitioner also notes that the District Court construed "biometric card pointer system" recited in both claims 1 and 19 "as a '[n]onlimiting preamble term with no patentable weight.'" *Id.* (citing Ex. 1033, 1). Neither party, on this record, disputes this construction, and therefore, to the extent necessary, we rely on the District Court's construction.

3. Defining

We note that Patent Owner proposes also, not a specific claim construction, but an interpretation that we should understand "defining" as meaning "setting" or "establishing." *See* PO Resp. 5–8 (Patent Owner arguing that "Petitioner repeatedly characterizes '*defining*, dependent upon the received card information' term with respect to *Bradford* as 'to find' or 'identifying.'"). Because the parties do not specifically construe the term

"defining," we address this issue in the context of the claim language as a whole, and the '039 specification, in our analysis below.

D. Ground 1: Claims 1, 2 19, and20 — Alleged Obviousness over Bradford (Ex. 1004) in view of Foss (Ex. 1005), and further in view of Yamane (Ex. 1006)

On the complete record now before us, Petitioner has shown by a preponderance of the evidence that claims 1, 2, 19, and 20 would have been obvious over Bradford, Foss, and Yamane.

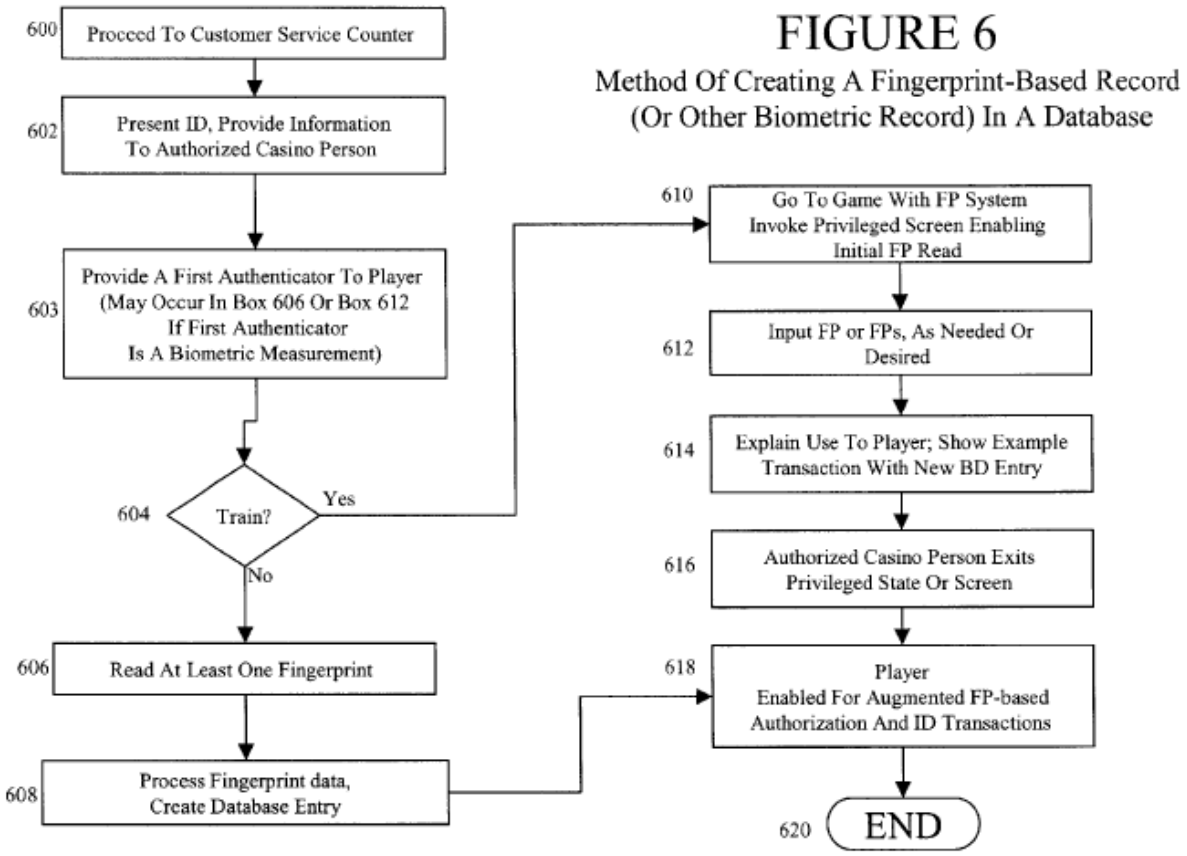
1. Bradford (Ex. 1004)

Titled "Player Identification using Biometric Data in a Gaming Environment," Bradford relates to player authentication systems and gaming machines using biometric data, which "allow a player to quickly and easily authenticate documents while remaining at game machines, [and] authenticate electronically based transfers into and out of accounts at game machines." Ex. 1004, Abstract, code (57).

Bradford discloses a gaming authentication system that uses at least two authenticators to identify a player, explaining "[t]he first authenticator may be one of many types, with a typical first authenticator being a player ID card, a voucher with a unique, encoded, and preferably encrypted numerical ID on it, a unique alphanumeric sequence, or an RFID tag." *Id.* at 3:6–10. Bradford discloses that "[t]he second authenticator will be based on a biometric reading. The present invention may use any biometric reading, although those providing reasonably high degrees of uniqueness are clearly preferred. It is expected that at the present time, the predominant biometric used will be based on fingerprints." *Id.* at 3:21–26.

Bradford further discloses a method for entering biometric data entry into a player ID database. *Id.* at 14:21–22. Bradford explains that "[a]

player identification database is also used, where an entry corresponding to a player comprises at least one record (typically, exactly one record), and the record has fields containing data, information, or pointers." *Id.* at 3:28–31. Bradford's Figure 6 is reproduced below.



Bradford's Figure 6, titled "Method of Creating a Fingerprint-Based Record [] in a Database," is a flow chart illustrating steps for creating a fingerprint, or other biometric data, as an entry in a database record. The process begins with a player going to a customer service counter at step 600 and then presenting identification and requesting an account at step 602. *Id.* at 14:23–28. At step 603, the player may be provided with a first authenticator, such as an ID card or voucher. *Id.* at 15:16–20. If a player desires training "[t]he attendant goes to a game with the present invention installed on it" where the player's biometric information is entered at step 612. *Id.* at 15:42–58.

Depending on whether a player needs training on how to operate a game at step 604, the player's biometric data, e.g., fingerprint data, is input to the database at either steps 606–608, or step 612. Once the first and second authenticators are stored, the player is enabled at step 618 to be subsequently verified and to operate a desired game device. *Id.* at 16:40–47.

2. Foss (Ex. 1005)

Foss is titled "Stored Value Card Account Transfer System" and describes various systems and methods for transferring funds between stored value card accounts of first and second customers. Ex. 1005, Abstract, code (57). Referring to Figure 8, Foss discloses in one embodiment "an enrollment process at merchant terminal 704 for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program." Ex. 1005 ¶ 86. Foss's Figure 8 is reproduced below.

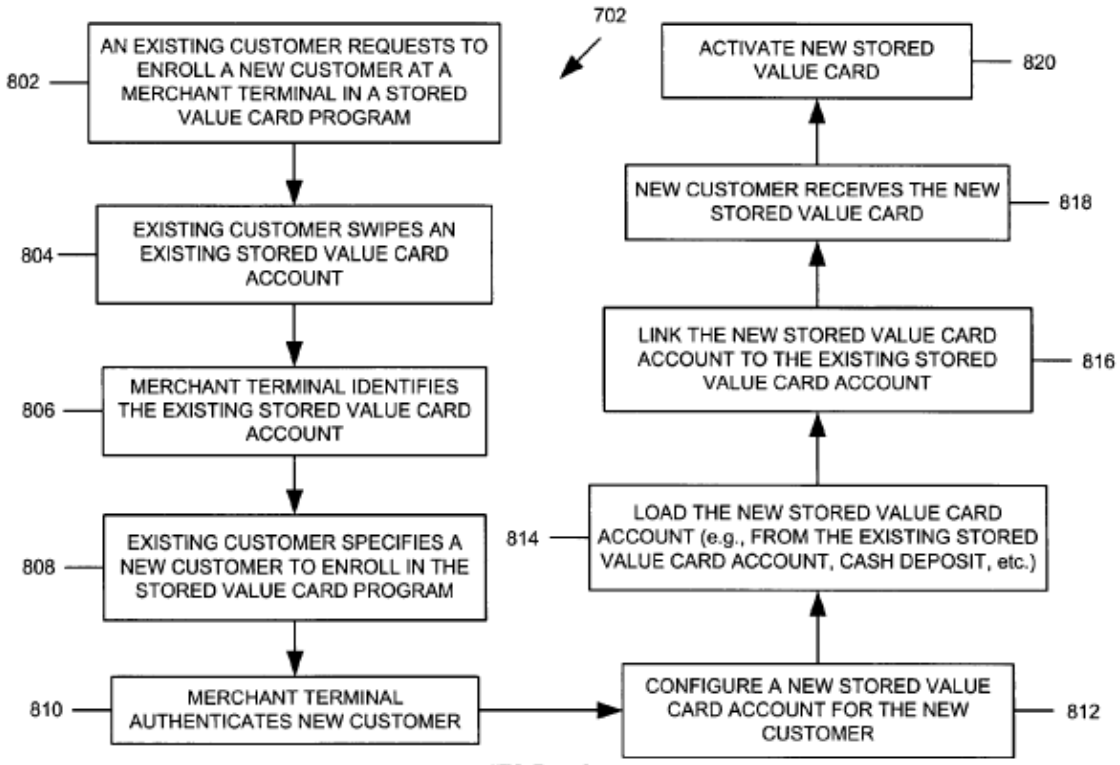


FIG. 8

Foss's Figure 8 is a flow chart illustrating steps for an existing customer having an existing stored value card and account to initiate enrollment of a new customer at steps 802–808. *Id.* ¶¶ 86–90. Foss explains that "[a]t block 806, merchant terminal 704 identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706." *Id.* ¶ 88.

Foss describes step 804 as part of a process by which existing customer 506 can swipe their card and begin an enrollment process for new additional customers, e.g., a family member. *Id.* ¶ 85. Foss's Figure 11 is reproduced below.

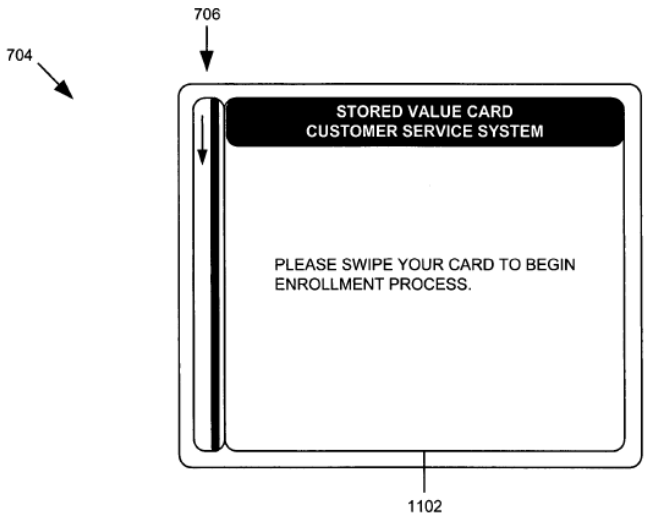


FIG. 11

Foss's Figure 11 "illustrates another input screen 1102 which prompts the existing customer 610 to swipe the existing stored value card 508." *Id.* ¶ 88. Foss explains that the new customer's account is added to the primary customer's account, and, after authentication of the new customer at step 810, Foss describes that a new stored value card is loaded with some monetary value and linked to the existing stored value card account at steps

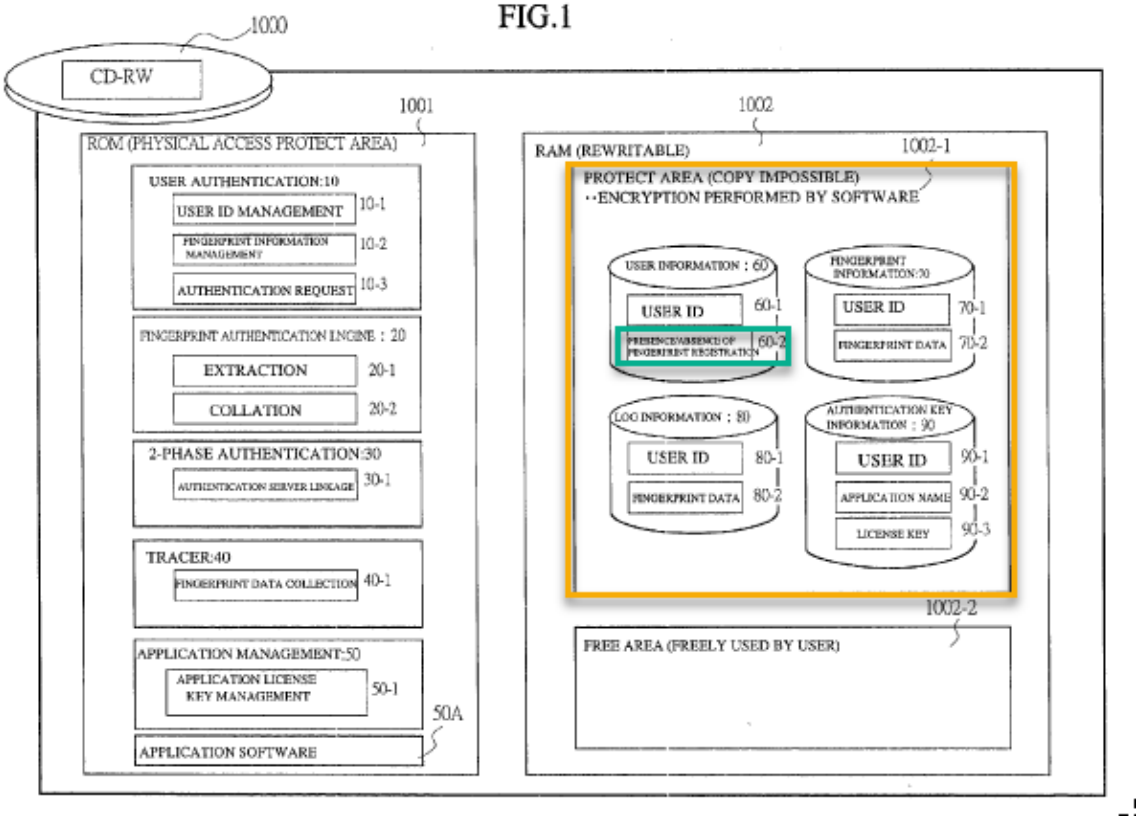
814, 816. *Id.*; *see also id.* at ¶ 90 ("At block 814, the existing customer 610 has the option of loading the new secondary stored value card account . . . with funds.").

3. Yamane (Ex. 1006)

Yamane is titled "Portable Recording Medium and Method of Using Portable Recording Medium" and discloses, for example, a CD-RW that requires identification of an authorized user before a user can access software stored on the CD-RW. Ex. 1006, Abstract. Yamane discloses specifically a user authentication program implemented as "software for performing a process of deciding a proper user on the basis of user fingerprint information input from the outside and fingerprint information which is registered in advance." *Id.* ¶ 33.

Considering Yamane's Figure 1, as annotated by the Board and reproduced below, Yamane describes user information 60 and fingerprint information 70 stored in a protect area 1002-1 (highlighted yellow) of rewritable area 1002 of CD-RW 1000. *Id.* ¶ 39.

FIG.1

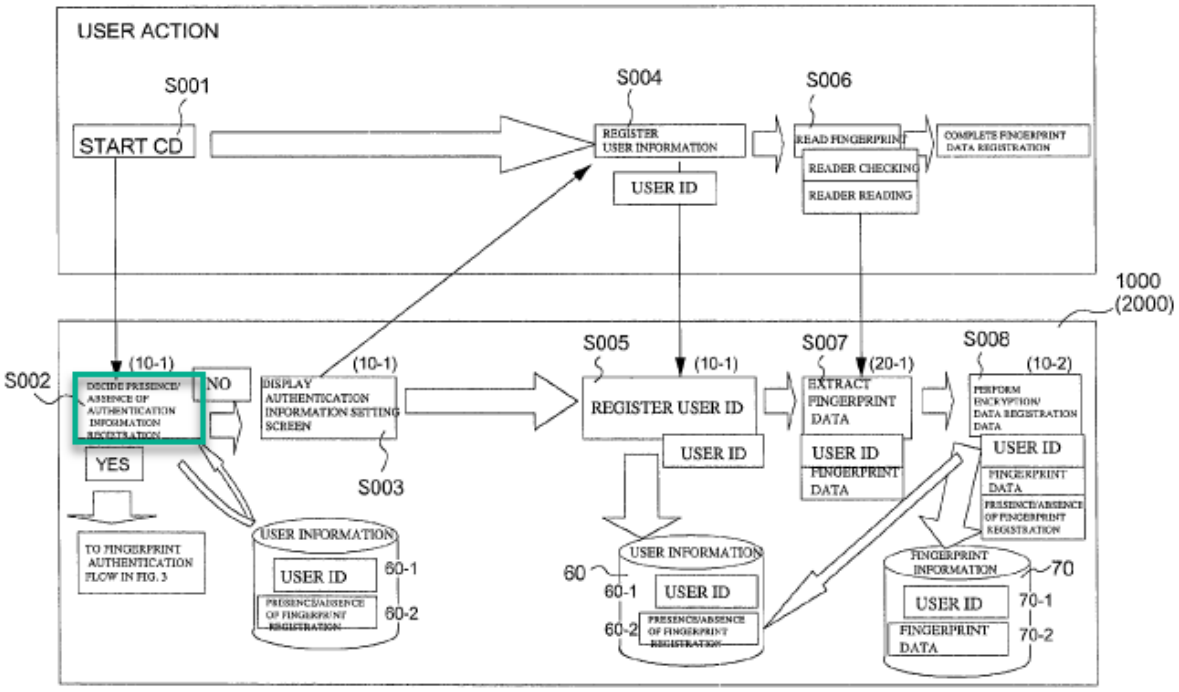


Yamane's Figure 1 illustrates user information 60 including User ID 60-1 and fingerprint registration presence/absence flag 60-2 (highlighted green). *Id.* ¶ 40. Referring to Figure 2, Yamane explains that

> [t]he user ID management function 10-1 of the user authentication program 10 decides whether a fingerprint has been registered or not with reference to the fingerprint registration presence/absence flag 60-2 of the user information 60 (step S002). If the fingerprint has not been registered, an authentication information setting screen for urging a user to register a fingerprint is shown to the user (step S003).

Id. ¶ 52. Yamane's Figure 2 as annotated by the Board is reproduced below.

FIG.2



Yamane's Figure 2 illustrates diagrammatically that following step S001, the start-up of CD, step S002 (highlighted green) detects the presence/absence of authentication information including presence/absence of fingerprint data 60-2. *Id.*

4. Independent Claim 1

(a) Petitioner's Arguments

Petitioner contends that a person of ordinary skill in the art would have understood Bradford, Foss, and Yamane in combination to teach all of the limitations of claim 1. *See* Pet. 5, 9.

i. Limitation [1Pre] – "A method of enrolling in a biometric card pointer system, the method comprising the steps of:"

Petitioner argues that even if the preamble is limiting, Bradford teaches such a method because Bradford describes enrolling a new user (a "player [seeking to use gaming devices] currently without an entry in [a]

player ID database") in the player ID database, the enrollment including "creation of an entry having biometric data in [the] player ID database." Pet. 9–12 (citing Ex. 1004, 3:50–54, 14:21–28, 15:16–24, 15:37–38, 15:48–58, 16:5–7, 16:21–32, 16:40–47, 22:25–56, Fig. 6). Petitioner explains that completion of Bradford's enrollment provides the player with "an entry in the player ID database corresponding to the player, having a first authenticator and a second authenticator useable by the player." *Id.* at 12 (citing Ex. 1004, 16:21–25, 16:40–47).

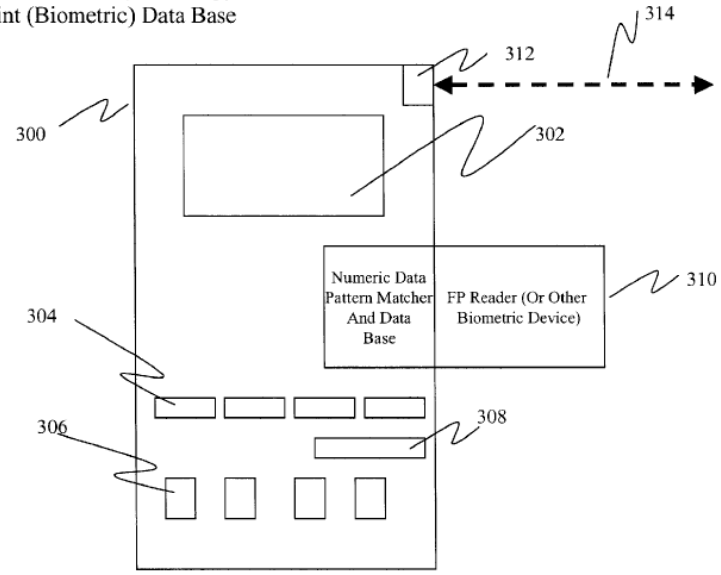
Petitioner argues that Bradford performs enrollment in "a biometric card pointer system" as claimed because "*Bradford* describes creating a player ID that is accessed using a player ID card" that includes the player's first authenticator, and the player ID (after enrollment) resides in the player ID database in which the enrolled players' entries include records having "fields containing data, information, or pointers. The records have fields corresponding to a first authenticator and a second authenticator, providing authenticator data therein or pointers to authenticator data." Pet. 9, 12–14 (citing Ex. 1004, 3:6–23, 3:28–36, 3:50–58, 5:36–54, 6:3–13, 15:16–20, 16:40–45, Fig. 6; Ex. 1003 ¶¶ 64–69).

ii. Limitation [1a] – receiving card information.

According to Petitioner, Bradford describes a magnetic strip card that may be inserted and read by a magnetic strip card reader to provide data of a "first authenticator" of a player. Pet 14–15 (citing Ex. 1004, 3:9–15, 6:4–6, 6:13–27, 8:22–31, 8:51–56; Ex. 1003 ¶¶ 70–72). In Bradford, the first authenticator is provided to the player during enrollment. *Id.* at 11–12 (citing Ex. 1004, 14:25–43, 15:16–24, 15:37–38, 15:48–63, 16:1–5, 16:26–32, Fig. 6).

Petitioner relies in part on Bradford's Figure 3, reproduced below, showing a "General Gaming Device" 300 having "first authenticator readers" 304. *Id.* at 14–15.

FIGURE 3
General Gaming Device Having A Fingerprint Reader (Or Other Biometric Reader) And Copy Of A Player Fingerprint (Biometric) Data Base



Bradford's general gaming device 300 includes, among other things, first authentication readers 304 and fingerprint reader 310. Ex. 1003, Fig. 3.

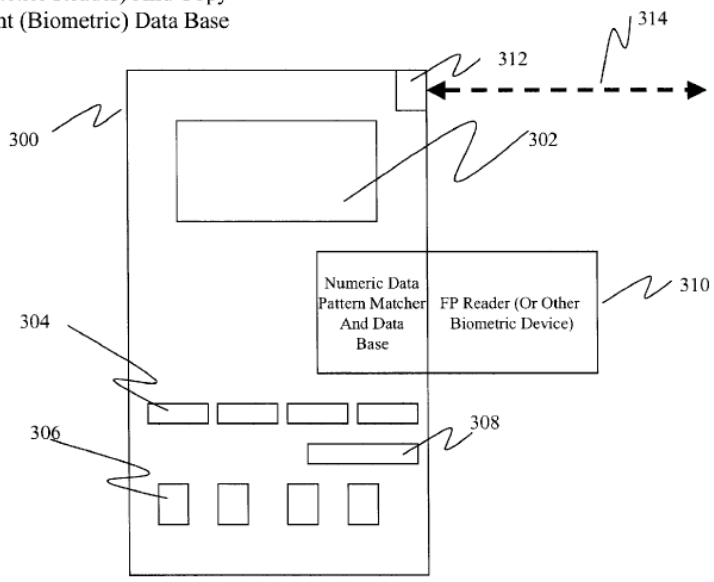
iii. Limitation [1b] – receiving the biometric signature.[7]

As shown above in Figure 3, Bradford describes a fingerprint reader 310 for receiving a fingerprint "biometric signature." Pet. 16 (citing Ex. 1004, 7:45–47, 8:22–28, 8:56–65, 10:30–40, Fig. 3; Ex. 1003 ¶¶ 64–65, 73–78). Petitioner relies in part on Bradford's Figure 3, reproduced below,

[7] As recited in claim 1, "the biometric signature" does not have antecedent basis. For purposes of our Decision, we assume this is incorrect and should be understood as "a biometric signature."

illustrating "General Gaming Device" 300 having an "FP Reader (Or Other Biometric Device)" 310."

FIGURE 3
General Gaming Device Having A Fingerprint Reader (Or Other Biometric Reader) And Copy Of A Player Fingerprint (Biometric) Data Base



Bradford's general gaming device 300 includes, among other things, first authentication readers 304 and fingerprint reader 310. Ex. 1003, Fig. 3.

iv. Limitation [1c] – defining, dependent upon the received card information, a memory location in a local memory external to the card.

Petitioner argues that Bradford discloses "a memory location, i.e., the second authenticator data field storing the second authenticator data [(biometric information, such as fingerprint data)], in a database, i.e., the player ID database." Pet. 23–24 (citing Ex. 1004, 6:3–30, 6:49–64, 15:59–63, 17:47–51, 17:18–22, 23:36–40). The biometric information is entered into Bradford's player ID database during enrollment—during which the two-level authentication system "creates the entry in the player ID database corresponding to th[e] player, associating the data corresponding to a first

and second authentic authenticator with this entry." Ex. 1004, 16:40–45; *see* Pet. 19–20 (citing Ex. 1004, 3:27–36, 14:21–28, 14:42–43, 15:16–23, 15:42–16:7, 16:21–26, 16:40–47, 23:36–40, Figs. 3, 6).

Petitioner argues that Bradford's first authenticator can be stored on "magnetic-strip cards" provided to the player during enrollment, or may be "an already existing player ID card." Pet. 18, 20–21, 24, 26 (citing Ex. 1004, 5:30–54, 6:3–13, 6:18–20, 13:23–33, 15:16–20).

Petitioner acknowledges that

> *Bradford* indicates the player entry is retrieved during the enrollment process because the player's second authenticator data is added to the player entry. *Bradford*, 15:60–63. *Bradford* does not indicate *how* the player entry is retrieved at the game device during enrollment.

Pet. 30 (citing Ex. 1003 ¶¶ 96–98). Petitioner then turns to Foss, explaining that

> *Foss* teaches "an enrollment process…for enabling a primary account holder (i.e., an existing customer 610) to enroll additional new customer(s) in the family stored value card program.". . . [t]o initiate enrollment, the customer is prompted "to swipe the **existing** stored value card" to "**continue** the **enrollment** process." The system "identifies the stored value card account associated with the existing customer 610. The stored value card account may be identified based on the data read from magnetic stripe 710 via card reader 706 . . ."

Id. at 27–28 (quoting Ex. 1005 ¶¶ 86, 88; citing Ex. 1003 ¶ 92) (citations omitted). Petitioner argues "[t]hus, *Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card." *Id.* at 28 (citing Ex. 1003 ¶¶ 93–94).

Petitioner argues that "*Bradford* in combination with *Foss* teaches that during *enrollment*, a user record stored in a database is retrieved by reading a card having unique user information thereon." *Id.* at 26 (citing Ex. 1003 ¶¶ 90–94). Petitioner asserts that a person of ordinary skill in the art would have looked to Foss because in Bradford "the enrollment process is not complete when the attendant and player move to the game device. The player entry needs to be retrieved for associating the biometric information." *Id.* at 29 (citing Ex. 1003 ¶¶ 95–98). Petitioner argues that "a very well-known and simple method of retrieving an account record is swiping a card with the account information, as indicated by *Foss*." *Id.* (citing Ex. 1003 ¶¶ 92–98).

Finally with respect to claim limitation 1(c), Petitioner submits that Bradford in combination with Foss teaches the defined memory location is "in a local memory external to the card" because Bradford's player ID database (which includes the enrolled players' ID entries) is stored locally at a game device. Pet. 19, 21, 31–33 (citing Ex. 1004, 8:51–65, 9:57–63, 14:21–28, 14:42–43, 15:16–23, 15:42–16:7, 16:21–26, 16:40–47, Figs. 3, 6; Ex. 1003 ¶¶ 83–85, 100–102).

v. Limitation [1d] – determining if the defined memory location is unoccupied.

Petitioner next argues that "*Bradford* (as otherwise modified by *Foss*) as modified by *Yamane* teaches determining if a flag is set indicating a memory location is occupied/no longer occupied, as claimed [in claim 1]." Pet. 33–34. Petitioner points out that the '039 patent "envisions a method in which determining if the defined memory location is unoccupied is performed by checking the status of a flag that 'can be set to indicate that the memory location in question is occupied' and 'reset to indicate that the

memory location in question is no longer occupied.'" Pet. 33 (citing Ex. 1001, 9:25–37). Petitioner then relies on Yamane for disclosing a "process of registering the fingerprint information of a proper user on [a] CD-RW 1000" by first "determining whether a fingerprint has been registered by reference to a flag." Pet. 34–36 (citing Yamane ¶¶ 33, 39, 41, 45–47, 49, 52–54, Figs. 1–2).

Petitioner argues that "*Bradford* (as modified by *Foss*) as further modified by *Yamane* renders obvious Claim 1(d)" because "*Yamane* already teaches the purpose of its flag is to 'decide[] whether a fingerprint has been registered or not,' thus indicating the flag determines if fingerprint data has been stored or not." Pet 38 (quoting Ex. 1006 ¶ 52) (citing Ex. 1003 ¶¶ 104–105, 109). Petitioner argues that "*Bradford* teaches a player entry is enabled once the second authenticator data field is populated to include the second authenticator data." *Id.* (citing Ex. 1004, 17:47-50). Therefore, according to Petitioner, a person of ordinary skill in the art would have been motivated "to modify the process of creation of the player entry to set a flag to determine if the memory location comprising the second authenticator data field is occupied with the second authenticator data or if such needs to be completed." *Id.* (citing Ex. 1003 ¶¶ 108–111).

vi. Limitation [1e] – storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

Petitioner argues that "*Bradford* (as modified by *Foss*) as further modified by *Yamane* renders obvious Claim 1(e)." Pet 39–40 (citing Ex. 1003 ¶¶ 108–114). According to Petitioner, a person of ordinary skill in the art would modify Bradford based on Yamane's teachings such that

> the fingerprint data corresponding to the second authenticator data [in Bradford] is stored at a memory location comprising the

> second authenticator data field [taught by Bradford] . . . When the memory location is unoccupied, as determined by the flag [taught by Yamane] in the modified *Bradford* system, the fingerprint data is then input into and stored in the memory location comprising the second authenticator data field, as taught by *Bradford*.

Pet. 40 (citing Ex. 1003 ¶¶ 108–114). Petitioner argues that a person of ordinary skill in the art would have combined Bradford's and Yamane's teachings for the reasons discussed with respect to claim limitation 1(d). *Id.* (citing Ex. 1003 ¶ 114).

(b) Patent Owner's Arguments

Focusing initially on limitation 1[c], Patent Owner argues that Petitioner has failed to prove that Bradford, Foss, and Yamane, alone or in combination, render obvious claims 1 and 19 because the cited art does not teach "defining, dependent upon the received card information, a memory location in a local memory external to the card" as recited in the claims. PO Resp. 7 (citing Ex. 1001, 12:33–34). Specifically, Patent Owner argues that "a memory location in a local memory which corresponds to, but is not contingent upon or determined by, the received card information is not 'dependent upon' under [Petitioner's] claim construction." *Id.* Also, with respect to limitations 1[d]–[e], Patent Owner asserts the prior art "does not teach 'determining if the defined memory location is unoccupied; and storing, if the memory location is unoccupied, the biometric signature at the defined memory location'" as required by these claims. *Id.* at 19.

Along with a focus on the claim limitations 1[c]–[e], Patent Owner presents additional arguments asserting that "a POSITA would not have looked to *Foss* in seeking to modify *Bradford*, and that "[a] POSITA would

not seek to combine *Bradford* and *Yamane* as [Petitioner] suggests." *Id.* at 17–19, 23–25. We address these arguments in turn.

> *(c) Whether the combination of Bradford and Foss teaches limitation [1c] "defining, dependent upon the received card information, a memory location in a local memory external to the card"*

Patent Owner argues that Bradford and Foss fail to teach the claimed "defining [a memory location]," which "a POSITA would consider . . . especially in the context of enrollment, to mean 'setting' or 'establishing,'" and "not finding or identifying something that has already been defined" and not "'pointing to' a memory location in which data is already stored," as Petitioner contends. PO Resp. 7–8 (citing Ex. 2001 ¶ 41); PO Sur-Reply 7. Patent Owner also asserts that a "temporal structure is implicit" in claim 1, which

> first requires card information be received. . . [a]fter, and only after, that card information is received can a memory location be defined. . . . [p]ut differently, **after** card information is received, the claim requires defining a memory location "contingent on" the received card information or that a defined memory location is "determined by" the received card information.

PO Resp. 8 (citing Ex. 2001 ¶¶ 42–43, 45; Ex. 2003, 15:12–16:6). Patent Owner submits that Dr. Sears, Petitioner's Declarant, admitted that claim 1's steps are framed by *a temporal structure* in which "the card information is obtained first, the memory location is defined by the card information second, and the biometric signature is stored in the defined memory location third." PO Sur-Reply 1–2 (citing Ex. 2003, 15:21–16:6; Ex. 1001, 12:29–38; PO Resp. 8; Pet. 26). Patent Owner observes that "Dr. Sears' admission . . . comports with the construction of the challenged claims put forth by Dr. Easttom, [Patent Owner's] expert. . . . [who] opined that the term

'defining' means 'setting' or 'establishing,' citing to the specification of the '039 Patent for support." *Id.* at 2 (citing Ex. 2001 ¶ 41; Ex. 1001, 2:64–67, 7:47–49); *see also* PO Resp. 7–8 ("in the context of the claim language, a memory location is set or established") (citing Ex. 2001 ¶¶ 41–43).

Despite not providing an explicit claim construction for "defining," most of Patent Owner's arguments center around the meaning of this word in the context of limitation [1c]. Therefore, we initially address the meaning of "defining" in the context of limitation [1c] as a whole.

i. The meaning of "defining"

Besides the agreed-upon construction of "dependent upon" as meaning "contingent upon or determined by," Patent Owner argues that "defining" also has a particular meaning, that is—"setting" or "establishing." PO Resp. 8. As issued, limitation [1c] reads:

> [1c] *defining*, *dependent upon* the received card information, a memory location in a local memory external to the card;

Ex. 1001, 12:33–34 (emphasis added). Given Patent Owner's proposed interpretation, we have:

> [1c] [setting or establishing], [contingent upon or determined by] the received card information, a memory location in a local memory external to the card;

We don't take issue with the alternative words specifically, but we observe that considering all the alternatives is repetitive and can lead to confusion because there are now 24, i.e., (4x3x2x1) permutations of the words/terms "setting," "establishing," "contingent upon," and "determined by," apparently deemed necessary to understand, what on its face, is not a particularly unwieldly claim recitation.

Claim limitation [1c] is best understood by reading the specification of the '193 patent, for example the Abstract, which reads:

> The disclosed Biometric Card Pointer arrangements store (207) a card user's biometric signature in a local memory (124) in a verification station (127) the first time the card user uses the verification station (127) in question. *The biometric signature is stored at a memory address (607) defined by the card information (605) on the user's card (601).* All future uses of the particular verification station (127) by someone submitting the aforementioned card (601) requires the card user to submit both the card and a biometric signature, which is verified against the signature stored at the memory address defined by the card information (605) thereby determining if the person submitting the card is authorized to do so.

Ex. 1001, Abstract, (57) (emphasis added).

We have no major issue with Patent Owner's interpretation of "defining" as also meaning "setting" or "establishing." Considering the abstract and the specification of the '039 patent, what "defining, dependent upon . . ." means as a whole, in the context of claim 1 and "a method of enrolling," is that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no memory location or address has been "set" or "established" for the fingerprint. When the fingerprint, and then the card, is provided to the system during enrollment, the card information provides data that establishes *where, e.g.,* at what memory location or address, the system will *store* the fingerprint data.[8] *See* Tr. 61:14–16 (Patent Owner's counsel arguing that "[w]e are saying it's defining a memory location into which the biometric data is going to be stored"). In all subsequent *verification* processes, when a

[8] We use the terms "memory location" and "memory address" interchangeably because, in terms of computer memory, an "address" is well-understood as "[a] number specifying a location in memory where data is stored." MICROSOFT COMPUTER DICTIONARY, 5th Ed. (2002) Microsoft Press.

person submits their card and fingerprint, the submitted fingerprint "is *verified* against the [fingerprint] stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so." *Id.* at 3:8–11; *see also* Tr. 36:23–37:3 (Patent Owner's counsel explaining during oral argument that "[i]f we look at these claims the way they're supposed to be looked at, as two discrete processes, then defining the memory location becomes very clear. It's what you're doing in the first instance to figure out *where you're going to store* the biometric data, and that is what is dependent upon the card information") (emphasis added).

Notably, because of the use of the term "defined" in claim 1 and dependent claim 2, Petitioner does not agree with Patent Owner's interpretation that "defining" means "setting" or "establishing." Pet. Reply 1–12. Petitioner argues that "[Patent Owner's] construction requires that 'defining' in claim 1 be construed differently than 'defined by' in claim 2." *Id.* at 10.

We acknowledge Petitioner's position, and take note of Petitioner's use of the words "find" and "identifying" to explain "define," but we do not have the same concerns.[9] Pet. Reply 3–5. In claim 1, following the

[9] In the context of these claims we do not understand "establish[ing]" and "identify[ing]" as any better or worse interpretations of "defining." Consider for example the following sentences:

-The witness *identified* the defendant as the person she observed in the store.

-The witness *established* the defendant as the person she observed in the store.

A reasonable reading of both sentences is quite similar—the witnesses' recollection is that she saw the defendant in the store. On the

"defining" step there is recited in past tense, "the defined memory location." Ex. 1001, 12:35, 39. Claim 2 recites "the memory location, . . . defined by the subsequently presented card information." *Id.* at 12:49–50. There is some merit to Petitioner's assertion here, because "defined" should be construed the same way in both claim 1 and claim 2. *See Phillips*, 415 F.3d at 1314 (explaining that "[b]ecause claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims"). We appreciate the argument because claim 2 recites "defined by the *subsequently* presented card information," meaning that for verification, following enrollment, this is not the first time the card is being presented. However, in claim 2 "the memory location" is the object of the preposition "defined by . . ." And, a reasonable reading of "the memory location . . . defined by" in claim 2 could also be understood grammatically similar to the past tense "defined memory location" in claim 1. Thus, consistent with claim 1, claim 2 can be understood as "the memory location . . . [established] by the subsequently presented card information." *Id.* Considering the meaning of the claims as a whole, as discussed above, Patent Owner's interpretation that "defining" means "setting" or "establishing" is not entirely inconsistent.

Importantly, and to make one thing clear, we do not understand that "defining . . . a memory location," or Patent Owner's alternative wording, "establishing" or "setting," means "[*creating*] . . . a memory location in a local memory." We bring this up because Patent Owner's counsel argued during the oral hearing that "there's nothing in Bradford that says you take

---

other hand, one would never state "the USPTO was identified in 1790," and would more likely say, "the USPTO was established in 1790."

that ID off the card *and create* the memory location based on that." Tr. 62:14–16 (emphasis added). Also, in the Patent Owner Sur-Reply, Patent Owner argues that "the memory location cannot already exist." PO Sur-Reply 2. While we might agree that "the memory location cannot [already be defined]," for the following reasons we do not agree that it "cannot already exist."

Coincident with the arguments raised by Petitioner above with respect to a consistent meaning of "defining," we point out that Patent Owner's interpretation of "defining" is somewhat of a moving target. Patent Owner argues that it is something more than "pointing to" or "finding," and perhaps means "creating." *See* PO Resp. 9 (Patent Owner arguing that "*Bradford*, notably, does not teach utilizing the first authenticator to create a player ID entry"). What Patent Owner's interpretation encompasses is not always clear. First, Patent Owner's expert's interpretation is that "defining" means "setting" or "establishing." *See id.* (Patent Owner stating that its expert "Dr. Easttom opined that the term 'defining' means 'setting' or 'establishing.'"); *see also* Ex. 2001 ¶ 41. Second, whatever Patent Owner's counsel is asserting as to the meaning of "defining," Dr. Easttom has not advanced any interpretation or construction that "defining" means "creating" a database location. Thirdly, Patent Owner has not pointed to any recitation of the word "create" in the specification of the '039 patent; nor has Patent Owner provided any technical explanation or reference to the written description as to what "creating" a memory location entails.[10] If anything, as Petitioner

[10] There is no technical or explanatory description in the '039 patent explaining *how* the card data creates or otherwise brings into existence a memory address. To the extent the written description lacks such technical

argues, the specification uses the word "points" and "pointer" to describe how the memory address or location is defined. For example, as shown in Figure 4 below, the "card data points to" an existing location 607 in a database "defined by card data."

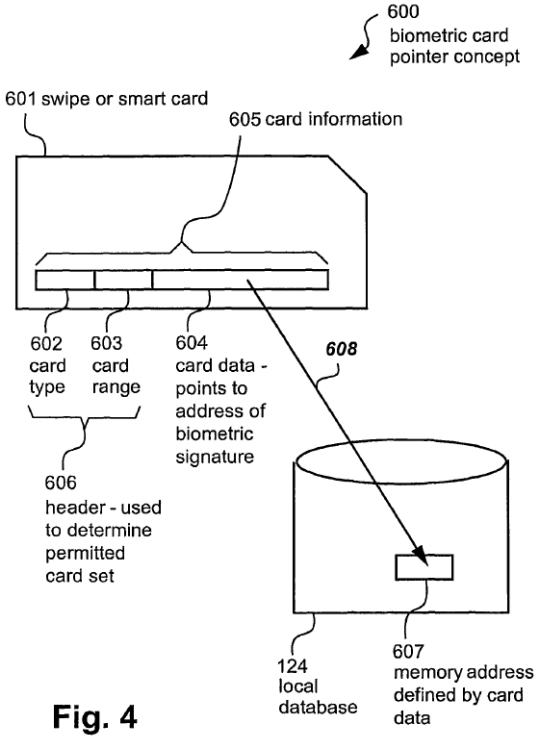


Fig. 4

Figure 4 states that as part of card information 605 the "card data [604] points to address of biometric signature." Ex. 1001, Fig. 4. Despite such disclosures throughout the specification, Patent Owner argues strenuously that "defining" does not mean simply "pointing to." PO Reply 7–17.

---

explanation, we do not have jurisdiction to address the issue of enablement. *See* 35 U.S.C. §112 ("The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.")

Regardless, we can give Patent Owner the benefit of the doubt that during an enrollment process the card data is provided for "setting" or "establishing" what memory location, or address, in the local database the fingerprint is to be stored. Even with this understanding, however, the card data does not actually *create* a memory location. The memory location already exists, it has just not yet been "set" or "established" by the card data as the memory location at which the fingerprint data is stored.

As expressed by claim 1 itself, this is the logically correct conclusion. Claim limitation [1d] recites "determining if the defined memory location is unoccupied." Ex. 1001, 12:35. If the card data somehow *created* a memory location, then there would be no reason to determine if the memory location were unoccupied. Indeed, Patent Owner's counsel stated during oral argument with respect to "defining" that "[t]he only logical use of that term is that defining means *to identify* a memory location into which the biometric data is going to be stored." Tr. 61:5–7 (emphasis added). During the oral hearing Patent Owner's counsel was specifically asked about the memory location:

> [THE BOARD]: What is a memory location? Is it a physical address within the memory?
>
> [PATENT OWNER'S COUNSEL]: Yes, Your Honor. That's one good way of looking at it. So you look at the memory structure for any standard-type memory, and it's just identifying an address in the memory location stored here.

Id. at 33:15–20. Indeed, when questioned further, Patent Owner's counsel was reluctant to use the word "create":

> [THE BOARD]: So as far as timing, you're saying the timing has -- I mean, it goes back to the definition of defining, right? I mean, you're saying the card information has to be used in order

> to create the locations of that information that stored in the database.
>
> [PATENT OWNER'S COUNSEL]: To define it, I would say, Your Honor.
>
> [THE BOARD]: Well --
>
> [PATENT OWNER'S COUNSEL]: Creating it. The memory location exists. It's going to be figuring out where to use your -- the answer to your question earlier, where -- what physical address in the memory --

Id. at 47:3–14. This discussion reveals the linguistic tangle Patent Owner faces in distancing the claimed "defining" step from Bradford and Foss.

Overall, in terms of "defining" and limitation [1c] as a whole, we understand that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been "defined," as in "set" or "established," in the memory for storing the fingerprint, until card information is received. Once the card information and fingerprint is received during enrollment, the card information provides data that establishes *where,* i.e., at what memory location or address, the system will *store* the fingerprint data.

ii. The temporal requirements of claim 1 and whether claim 1 "first requires card information be received. . . After, and only after, that card information is received can a memory location be defined"

Patent Owner contends that a "temporal structure is implicit" in claim 1, which "first requires card information be received. . . [a]fter, and only after, that card information is received can a memory location be defined." PO Reply 8 (citing Ex. 2001 ¶ 45).

We agree that there is a temporal aspect to claim 1. We agree that the biometric signature, e.g., a fingerprint, is not *stored* (step [1e]) until after

receiving the card information (step [1a]). Ex. 1001, 12:29–38. This is because it is the card information that tells the system where, i.e., establishes (defines) a specified memory location to store the fingerprint at step [1c]. What we do not agree with, as Patent Owner appears to intend with this argument, is that a memory location does not already exist, or is somehow created only upon presentation of the card information. Indeed, as we explain below, the limitations of claim 1 do not exclude an existing user or player record entry from being a memory location in a database where the fingerprint is stored.

For one thing, claim 1 recites specifically "[a] method . . . *comprising* the steps of . . ." *Id.* at 12:29–30. It is well-settled that "comprising" is an open-ended term and "[i]n the patent claim context the term 'comprising' is well understood to mean 'including but not limited to.'" *CIAS, Inc. v. All. Gaming Corp.*, 504 F.3d 1356, 1360 (Fed. Cir. 2007). Patent Owner has not pointed to any persuasive part of the specification of the '039 patent describing that a user or player record cannot exist prior to the use of the card for "defining . . . a memory location" where a biometric signature is to be stored. We agree that *prior* to use of the card *a memory location for storing a biometric signature* is not "established" or "set," but we do not agree that the memory location does not exist or that the language of claim 1 excludes the existence of a database record, and even a database record including user record information in the memory location.[11]

[11] "[I]n general, a patent claim reciting an apparatus 'comprising' various components merely means that the apparatus 'includ[es] but is not limited to' those components." *Rothschild Connected Devices Innovations, LLC v. Coca-Cola Co.*, 813 F. App'x 557, 562 (Fed. Cir. 2020) (nonprecedential) (citations omitted).

Secondly, during oral argument, Patent Owner's counsel confirmed that "enrollment" in the context of claim 1 requires the "receiving card information" to *identify* a memory location for storing a biometric signature:

> [THE BOARD]: But claim 1 doesn't say that the card data defines it. It says defining dependent upon the received card information. It's --
>
> PATENT OWNER'S COUNSEL]: Your Honor, going -- yes, Your Honor, but going back to the conversation you and I had during my argument in chief, if you look at what dependent upon means, it's contingent upon. *You can't have the memory location before you have the card data*.
>
> . . .
>
> [PATENT OWNER'S COUNSEL]: . . . But it is the card information that determines what the memory location is going to be. So when Ms. Bailey said that any time a card is used to locate information in memory, that is defining the memory location, that simply isn't true, according to the definition that [Petitioner] proposed. But more importantly, when we look at claim 1, it talks about an enrollment process. If defining were to include simply identifying information where the data is stored, according to the order of steps in claim 1, the biometric information isn't stored yet, so what would it be defining?
>
> There's nothing to define at that point. There has been no storage of that biometric information, according to [Petitioner's] definition. *The only logical use of that term is that defining means to identify a memory location into which the biometric data is going to be stored.*

Tr. 59:11–61:14 (emphases added).

Keeping in mind the meaning of limitation [1c] based on the claim language and specification, the interpretation that stays true to the claim language and most naturally aligns with the patent's description of the invention is that, during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory and no

memory location or address has been established in the memory for the fingerprint. When the card is provided during enrollment, the card information provides data that establishes *where,* i.e., at what memory location or address, the system is *to store* the fingerprint data." Section II.4.(c)(i).

Therefore, based on our determination of the proper interpretation of "defining," we agree with Patent Owner's counsel that at limitation [1c] "according to the order of steps in claim 1, the biometric information isn't stored yet." Tr. 60:25–61:1. We also agree, based on all the evidence before us, and as Patent Owner's counsel argued, that "[t]here has been no storage of that biometric information, . . . *[t]he only logical use of that term is that defining means to identify a memory location into which the biometric data is going to be stored*." Tr. 61:5–7 (emphasis added). On the complete record before us, Patent Owner's explanation that "defining means to *identify* a memory location" is entirely consistent with Dr. Easttom's explanations, and our interpretation that the card information establishes *where,* i.e., a memory location or address, the system is to *store* the fingerprint data.

Therefore, based on the proper interpretation and understanding that the meaning of "defining" includes "sets" or "establishes," we can agree with Patent Owner that "[a]fter, and only after, that card information is received can a memory location be defined" for the biometric signature. PO Reply 8 (citing Ex. 2001 ¶ 45).

(d) Obviousness of limitation [1c] based on Bradford and Foss

We note that the parties are somewhat in agreement about Bradford's disclosure, that is—Bradford discloses a casino attendant, for example,

providing a player entry in the player ID database *prior* to a first use of the first authenticator, e.g., a player ID card. Pet. 11 (citing Ex. 1004, 14:25–43, Fig. 6, 15:37–38); *see also* PO Resp. 2 (Patent Owner asserting that "the experts for each party agrees, the database entry in the prior art (which Apple's expert characterized as 'the memory location') is created **before** card information is received").

However, we do not find that the player ID database being created prior to use of the player ID card in Bradford is excluded from the scope of claim 1. As discussed above, the temporal nature of claim 1 relates to "receiving card information," "receiving the biometric signature," and then "storing . . .the biometric signature" dependent, i.e., contingent on the card information. As we established, claim 1 does not recite, nor does "defining" mean, that a memory location cannot exist prior to use of the card as Patent Owner argues. What claim 1 requires is the initial "establishment" or "setting" of a memory location for storage of the fingerprint. As we discussed above, claim 1, including limitation [1c], would have been understood by a person of ordinary skill in the art, to mean that during an *enrollment* process, the claimed "biometric signature," e.g., a fingerprint, is not yet stored in the memory, and no memory location or address has been established in the memory for the fingerprint. Once the card is provided during enrollment, the card information provides data that establishes *where,* i.e. at what memory location or address, the system is to store the fingerprint data.

Petitioner and Patent Owner also appear to agree that Bradford does not expressly disclose *how* a player entry is located or retrieved during an exemplary *enrollment* at a game device in the casino prior to recording the new player's fingerprints in the player ID database. *See* Pet. 26–27

(Petitioner arguing that "*Bradford* teaches the enrollment process that began at the customer service counter is continued and completed at the particular game device but is not express about *how* the previously-created player entry in the player ID database is located and accessed for completion on the particular game device"); *see also* PO Resp. 17–18 (Patent Owner arguing that "[Petitioner] is correct that *Bradford* does not teach how a player entry is retrieved during the creation of that player's ID entry").

To this end, Petitioner argues that "*Bradford* . . . is not express about how the previously-created player entry in the player ID database is located and accessed [during enrollment] for completion on the particular game device." Pet. 26–27. Petitioner submits that "*Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card"—in other words, "a continuation of an enrollment process via presentation of a card to a card reader." Pet. 27–28 (citing Ex. 1005 ¶¶ 86, 88, Figs 7–8; Ex. 1003 ¶¶ 92–94). Petitioner asserts that based on Foss "[a] POSITA would have found it obvious that a convenient and expected method for locating the player entry associated with the player ID on the card would have been to read the player ID from the card via the card reader [(as described by Foss)] on the particular game device [(where enrollment occurs in Bradford)]." Pet. 27 (citing Ex. 1003 ¶¶ 92–94); *see also* Pet. Reply 19 ("The Petition maps 'receiving card information' by modifying *Bradford* via *Foss* to swipe *Bradford's* player ID card using *Bradford's* card reader.").

On the other hand, Patent Owner contends that "*Foss* does not cure the deficiencies of *Bradford* in failing to teach" the "defining" limitation. PO Resp. 9. Patent Owner contends Foss is deficient (and does not cure Bradford) for multiple reasons, which we discuss in turn below.

Patent Owner argues Foss is deficient because "*Foss* does not teach enrolling a single-user account by utilizing received card information to define a memory location"; "[i]nstead, *Foss* is directed towards expanding an existing customer account." PO Resp. 9–10 (citing Ex. 2001 ¶ 53; Ex. 1005 ¶¶ 85–86, 88, Figs. 7–8). Relatedly, Patent Owner argues Foss's description of swiping an existing card to enroll additional users (and create respective multi-user accounts) "would be illogical when applied to the enrollment of an individual account" because "unlike [Foss's] family card program, *there would be no existing account to reference* when enrolling an individual" (in Bradford). PO Resp. 11 (emphasis added) (citing Ex. 1005 ¶ 88, Fig. 10).

Petitioner replies that the obviousness analysis relies on Foss "only . . . for clarification of receiving card data during an *enrollment* process" to "locat[e] a user's record to add additional information." Pet. Reply 23–24 (citing Pet. 2, 17, 25–30); *see* Pet. 26 ("*Bradford* in combination with *Foss* teaches that during enrollment, a user record stored in a database is retrieved by reading a card having unique user information thereon."); *see also id.* at 28 ("*Foss* teaches, during an enrollment process, identifying an account associated with a user by reading account information stored on a magnetic stripe of a card.") (citing Ex. 1003 ¶¶ 90–94).

Petitioner's declarant, Dr. Sears, explains in detail how Petitioner's obviousness analysis relies on Foss for using a card during an enrollment process to identify an account associated with a user by reading information stored on the card using a card reader. Ex. 1003 ¶¶ 90–98. Dr. Sears explains that the Bradford-Foss combination "modif[ies] *Bradford's* enrollment process to include swiping the player ID card at the game device to retrieve the associated player ID entry, as taught by *Foss*." *Id.* ¶ 95.

Based on Dr. Sears' testimony, Petitioner concludes that, "[r]egardless of the type of account in which a user is enrolled, *Foss's* teachings regarding locating a user's record to add additional information is relevant to the same process being performed in *Bradford*." Pet. Reply 23.

We agree with Petitioner's assessment and credit Dr. Sears' testimony. Both Foss and Bradford describe an enrollment process in which a customer's existing database record is established as a location for storing additional information, e.g., a player's data and information entered by an authorized person into the player ID database at Bradford's step 602, a player's first authenticator data that is read and thereafter kept in the database in Bradford, and a customer's stored value card account/primary account in Foss.

Although Patent Owner contends that, contrary to Foss, there is no existing customer in Bradford and "there would be *no existing account to reference* when enrolling an individual" in Bradford (*see* PO Resp. 10–11 (emphasis added)), Bradford actually discloses and teaches that *some of the customer's information*—such as "the initial data from the player [entered by an authorized person] into the database"—occurs before "the attendant asks the player if they need training" and enters fingerprint data. Ex. 1004, 14:21–31, 15:29–31.

> As explained in detail by Petitioner's declarant, Dr. Sears,
>
> *Bradford* teaches that during enrollment a player's entry is created and stored with first authenticator data, the player is provided a player ID card with the first authenticator data, the casino attendant and player move to a game device for training and entry of the player's fingerprint information.

Ex. 1003 ¶ 90 (citing Ex. 1004, 15:42–16:20). We find Dr. Sears' testimony credible and supported by the disclosure of Bradford, and we are persuaded

that a customer's initial information (i.e., the information saved in Bradford's player ID database during enrollment before recording the biometrics) represents account information that is available for subsequent retrieval (e.g., retrieval during Bradford's recording of the biometrics). Pet. 19–20, 26, 29–30 (citing Ex. 1003 ¶¶ 83–85, 90–98).

We find little weight in Patent Owner's argument that Foss cannot be relevant to Bradford because "*Bradford* does not contemplate creating multi-user accounts [as in Foss]." PO Resp. 11. Just as Bradford's completion of enrollment, including setting up a user account, is *in progress* until the biometric signature is added to the account, Foss's family stored value card account 600 is an in-progress enrollment process being completed when a secondary stored value card account (e.g., 604) is added thereto. *See* Ex. 1005 ¶¶ 85–86, 88, Figs. 6, 8; Pet. Reply 24 ("In the combined, modified system, an account exists prior (per *Bradford*) to receiving the card information (per *Foss*), whether or not the biometric signature has yet been stored for that account.").

Overall, we are persuaded that Petitioner and Dr. Sears have shown a preponderance of evidence that a person of ordinary skill in the art, who was aware of all the prior art in the relevant field, would have recognized that Bradford does not expressly disclose *how* a user's ID information entry would have been retrieved from a database. Petitioner and Dr. Sears have further shown that, in turn, the person of ordinary skill in the art would have looked to Foss, which more specifically teaches that information on a user's ID card was a known way to define, that is to "establish" or "set" a memory location, for example with the user's player ID record entry, where a user's input of a second authenticator, e.g., a fingerprint, would be stored.

We acknowledge Patent Owner's extensive arguments regarding Bradford's failure to teach (alone, or in combination with Foss) "first receiving card information and then defining a memory location based on that received card information." *See* PO Resp. 9–17; PO Sur-Reply 3–4, 7–10. For example, Patent Owner argues that Petitioner's expert, Dr. Sears, "testif[ied] that *Bradford* teaches a process in which the steps are reversed - a memory location is defined before any card information is received." PO Sur-Reply 3 (citing Ex. 2004, 31:12–18). We do not agree that Dr. Sears' testimony conflicts with claim 1. When claim 1 is properly interpreted, as we have addressed herein, the creation of a player account in Bradford, or Foss, prior to receiving the card information does not preclude subsequently identifying a memory location (among preexisting memory locations/addresses within the preexisting player ID database) and establishing that memory location as the location where new biometric data, e.g., a player's fingerprint, is going to be stored. *See* Pet. Reply 23–24; Pet. 26–28. That is, creating a player account in Bradford does not preclude subsequently "defining, dependent upon the received card information, a memory location," as recited in claim 1. Pet. Reply 23–24; Pet. 26–28.

In other words, we do not agree that claim 1 excludes the existence or creation of a player account record in "a memory location" prior to receiving card information. Claim 1 precludes the establishment or setting of a memory location for the "biometric signature" prior to receiving card information, but "defining" does not mean that the memory location is created or somehow brought into existence only after "receiving card information."

Considering our claim interpretation and the parties' interpretations and constructions of limitation [1c], we have explained why Patent Owner's

arguments do not undermine Petitioner's contentions and supporting evidence, and why we agree with Petitioner that a person of ordinary skill in the art would have understood that the Bradford-Foss combination teaches all the elements in limitation [1c]. Specifically, we are persuaded on the complete record now before us that where Bradford discloses an enrollment process including receiving card information and biometric information, but does not describe specifically *how* to store the biometric information, Foss teaches how, i.e., using card data to define, that is—to establish or set a memory location, e.g., the player's user account, for storage of the biometric information in a local memory.

(e) Whether Bradford and Foss are properly combined.

Patent Owner contends that a person of ordinary skill in the art would not have combined Bradford and Foss. PO Resp. 2–3, 17–19. In particular, Patent Owner argues an ordinarily skilled artisan would not have looked to *Foss* because "*Bradford* teaches the attendant's card being placed in the machine in order to access the privileged screen in which the player's entry is retrieved to complete registration" such that the player's first authenticator card "could not, then, be 'read by a card reader to retrieve the stored first authenticator data.'" *Id.* at 18.

We do not agree with Patent Owner. Rather, we find Petitioner's position persuasive that "*Bradford* expressly envisions embodiments not 'requiring' the attendant's card staying in the machine during enrollment." Pet. Reply 19–20, 22–24 (citing Ex. 1004, 14:31–41, 14:28–37). Bradford, for instance, teaches a casino attendant accessing privilege screens using an RFID tag which does not require the casino attendant's card remaining in the machine. *See* Ex. 1004 14:28–37 (Bradford describing that "[i]n order to

open the privileged screens allowing data entry, the authorized casino personnel will be required to use their own employee identification cards (badges, **RFID** tag, . . .")). Importantly, we credit the testimony of Petitioner's expert, Dr. Sears, who testifies that to a person of ordinary skill in the art, "swiping the player ID card would have been a logical, fast, and simple method of retrieving the player ID entry." Ex. 1003 ¶ 96. Dr. Sears relies on express teachings in Foss, testifying that "*Foss* also teaches that the 'existing customer 610 swipes the existing stored value card 508 to further continue the enrollment process,' and the 'stored value card account may be identified based on the data read from the magnetic stripe 710 via card reader 706.'" *Id.* ¶ 94 (quoting Ex. 1005 ¶ 88).

Dr. Sears testifies further that "modifying *Bradford* according to the teachings of *Foss* would have had a reasonable expectation of success" because "*Bradford* teaches both hardware and software used for reading player account information from a card's magnetic strip" as well as "programmed functionality for matching a unique data sequence stored on a card as first authenticator data to the first authenticator data in the player entry and thus retrieving a corresponding player entry." *Id.* ¶ 98. Dr. Sears testifies that

> modifying *Bradford* to swipe the player ID card having the first authenticator data to retrieve a partially-completed player entry would have been applying the known technique of swiping a card that has a magnetic stripe with account information (taught by both *Bradford* and *Foss*) to a known card reader device (taught by *Bradford*).

Id. ¶ 97. Thus, Dr. Sears concludes that "[s]uch a modification would have yielded the predictable result of retrieving the player entry that matches the first authenticator data read from the player ID card." *Id.*

We further credit Dr. Sears' testimony that a person of ordinary skill in the art: (i) would have had a reason to combine the teachings of Bradford with Foss, which both relate to setup as well as augmentation of users' accounts; and (ii) would have known how to employ a customer's authenticating card to identify the customer using a card reader during an enrollment process, so that the teachings of Foss would have been applicable to Bradford's two-factor enrollment process. Ex. 1003 ¶¶ 62, 90, 92–102. Patent Owner's observation that "*Bradford* . . . requires biometrics for at least the second authenticator," while "none of [Petitioner's] cited portions [of Foss] contains a reference to biometrics" (PO Resp. 19), does not explain why a person of ordinary skill in the art would not have recognized, as suggested by Foss, that the authenticating card could still be used to retrieve a partially-completed player entry in Bradford, before the processing of biometrics. *See* Ex. 1003 ¶ 98 (Dr. Sears testifying that swiping a user ID card to retrieve a user entry "according to *Foss's* teachings encompasses performing a known look-up process for the player entry during the enrollment for the two-level authorization process, as taught by *Bradford*"). The test for obviousness is what the combined teachings of those references would have suggested to those of ordinary skill in the art. *See In re Mouttet*, 686 F.3d 1322, 1331 (Fed. Cir. 2012) ("A reference may be read for all that it teaches, including uses beyond its primary purpose.").

(f) Whether the combination of Bradford, Foss, and Yamane teaches limitation 1(d) "determining if the defined memory location is unoccupied"

According to Patent Owner, Yamane's "protect area 1002-1 of a rewritable area 1002 is a *pre-defined* memory location, not a memory location which is defined by, contingent on, or determined by, any other

information, much less received card information as the claim requires." PO Resp. 20 (emphasis added). Patent Owner argues that "the inclusion of *Yamane* would seek to determine if a specific, pre-defined memory location was unoccupied," which is distinct from the claimed memory location "defined dependent upon received card information." *Id.* at 20–21 (emphases added) (citing Ex. 2001 ¶ 57); *see also* PO Sur-Reply 12–13 ("*Yamane* teaches checking whether a specific, pre-defined memory location is occupied via a flag, whereas the claim describes "determining if *the defined memory location* is unoccupied").

In response, Petitioner points out that "the Petition . . . relies on *Yamane* only for a method of checking a fingerprint presence flag." Pet. Reply 26 (citing Pet. 33–37). This argument, Petitioner asserts, "is improperly engaging in bodily incorporation of features from a secondary reference into a primary reference." *Id.*

We find Petitioner's arguments and evidence persuasive because Petitioner relies upon Bradford and Foss for the claimed *function* of "defining . . . a memory location," into which the biometric signature is eventually stored. *See* Pet. 17 ("*Bradford* in combination with *Foss* teaches Claim 1(c)."); *see also id.* at 19 (quoting Ex. 1004, 40:46–48) ("*Bradford* teaches an enrollment process "for the creation of an entry having biometric data in a player ID database."). And, besides bodily incorporating features, i.e., a memory location of Yamane, that Petitioner does not assert with respect to the "defining" limitations in [1c], Patent Owner's argument conflates the "defining" step in limitation [1c] with [1d]. Limitation [1d] follows [1c], and simply "determin[es] if the memory location is unoccupied." Ex. 1001, 12:35.

Secondly, and with respect to Yamane itself, claim 1 is a method claim, whereas Patent Owner's argument is based upon a specific type of "protect area" memory, e.g., a structural aspect of memory. PO Resp. 20. Apart from the assertion that a "protect area" is "pre-defined," Patent Owner's argument does not explain *how* the memory is defined, or pre-defined for that matter, except from the functional vantage point of the "received card information." In other words, the claim does not limit what type or structure of external local memory can be set or established as a memory location for the biometric signature, and Patent Owner does not explain sufficiently why "received card information" could not functionally establish a "protect area" of an external memory structure, as a memory location to store data, such as the biometric signature.

> Specifically considering limitation [1d], the Petition explains that
>
> User information 60 and fingerprint information 70 are stored in a protect area 1002-1 of a rewritable area 1002 of the CD-RW. *Yamane*, [0039], FIG. 1. During a "registration process" (i.e., enrollment), fingerprint information 70 comprising user ID 70-1 and fingerprint data 70-2 are obtained.
>
> . . .
>
> *Yamane* discloses a "process of registering the fingerprint information of a proper user on the CD-RW 1000." *Yamane*, [0049], FIG. 2. *Yamane* expressly discloses determining whether a fingerprint has been registered by reference to a flag. . .

Pet. 34–37. Regardless of whether "protect area 1002-1" is "pre-defined" and whether the claim language means something different, Petitioner relies on Yamane mainly for "determining" whether the memory location is occupied or not, based on the presence or absence of a flag. *See* Ex. 1003 ¶ 104 (Dr. Sears explaining that "*Yamane* teaches that during an enrollment

process, storage of a fingerprint at a memory location is determined based on the presence or the absence of a flag").

To the extent necessary, we also do not find that Petitioner's Bradford-Foss-Yamane combination relies on a memory area that is "a pre-defined" memory location as Patent Owner asserts. *See* PO Resp. 20. Patent Owner appears to contrast "pre-defined" with "card-defined." *Id.* at 21. Yamane describes "protect area 1002-1" as a "rewritable area 1002" that is "a data storage region [of CD-RW 1000] . . . in which data can be rewritten," protect area 1002-1 being an area "in which written data is protected by encryption performed by a software." Ex. 1006 ¶¶ 29, 31. Thus, the term "protect" in Yamane (i.e., in "protect area 1002-1") refers to a data storage region/memory portion for which data written therein is "protected by encryption performed by a software," not to a memory portion that is somehow functionally "pre-defined" so as to exclude the storage of information based on separate card data. *See* Ex. 1006 ¶ 31(Yamane explaining that "[t]he rewritable area 1002 is constituted by a protect area 1002-1 in which written data is protected by encryption performed by a software").

Patent Owner next contends that an arrangement produced by the Bradford-Foss-Yamane combination "would be immaterial to *enrollment*, as the *pre-defined memory location, prior to such enrollment, would necessarily be unoccupied*." PO Resp. 21 (citing Ex. 2001 ¶ 58). Besides the fact that Petitioner is not relying on Yamane's alleged "pre-defined" memory location but on the local memory "player ID database" disclosed by Bradford, claim 1 does not condition the "defining" step [1c] on prior knowledge or information as to whether the "defined" memory location is occupied or not. Pet. 20. Limitation [1d] recites "determining if the defined

memory location is unoccupied"—irrespective of any specified knowledge regarding occupancy of the local memory's memory locations. *See* Ex. 1001, 12:29–38.

Patent Owner further argues that Petitioner's reliance on "system-wide audits for records missing biometric signatures" is unsupported by Bradford, Foss, or Yamane, and "[e]ven if a POSITA would have had it in mind to run system-wide audits, these audits would be worthless when enrolling individual players, as in *Bradford*." PO Resp. 21 (citing Ex. 2001 ¶¶ 57–59).

Even if Patent Owner's position here is correct, the Petition's discussion of the Bradford-Foss-Yamane combination is not limited to a rationale based on system-wide audits. *See* Pet. Reply 26. Rather, the Petition (and supporting evidence) include "lengthy discussion regarding obviousness of modifying *Bradford* to include *Yamane's* flag to indicate the memory is unoccupied," for example referencing "the benefit to *Bradford's* system to determine if an entry in the player ID database is 'complete, valid, or enabled' and that setting flags was well-known." *Id.* at 26–27 (citing Ex. 1003 ¶¶ 103–112; Pet. 39 (citing Ex. 1001, 17:14–26)). As discussed *infra*, we find that Petitioner provides persuasive rationale for combining the teachings of Yamane with those of Bradford and Foss. Pet. 37–39; Ex. 1003 ¶¶ 108–112.

Considering all the evidence and the parties' arguments before us, we are persuaded that Petitioner has shown a preponderance of evidence that Yamane, in combination with Bradford and Foss, teaches limitation [1d].

(g) Whether the combination of Bradford, Foss, and Yamane teaches limitation [1e] "storing, if the memory location is unoccupied, the biometric signature at the defined memory location"

According to Patent Owner, similar to the arguments for limitation [1d], "*Bradford* in view of *Yamane* does not teach the 'storing' limitation because *Yamane* relies on a pre-determined memory location whereas the location of *Bradford's* putative 'defined memory location' is, in actuality, undefined." PO Reply 21 (citing Ex. 2001 ¶ 57); *see also* PO Sur-Reply 13. We find this argument unpersuasive because, as discussed *supra*, Petitioner relies on Bradford, not Yamane, for "defining . . . a memory location."

Patent Owner next argues that "even when considering *Bradford* in combination with *Foss*, the location at which the biometric signature is stored *remains unclear*" such that "[i]t cannot be, then, that [Petitioner's] variety of references renders obvious the claimed 'storing.'" PO Resp. 21–22 (emphasis added) (citing Ex. 1001, 12:37–38, 16:10–11).

This is unpersuasive because Petitioner relies upon Bradford's "player ID database" as the memory location. Pet. 20. Interestingly, one could just as easily make this argument about claim 1, which also does not describe any specific memory location, requiring only that the memory location is "defin[ed], dependent upon the received card information." In any event, in response, Petitioner points out persuasively that the Petition "provided lengthy discussion regarding obviousness of modifying *Bradford* to include *Yamane's* flag to indicate the memory is unoccupied." Pet. Reply 26 (citing Ex. 1003, ¶¶ 103–112).

Yamane describes that "[u]ser information 60, fingerprint information 70, log information 80, authentication key information 90, and the like are stored in the protect area 1002-1 of the rewritable area 1002." Ex. 1006

¶ 39. Yamane then explains that "[t]he user information 60 is constituted by pieces of information such as a user ID 60-1 and a fingerprint registration presence/absence flag 60-2 which are uniquely given to respective users." *Id.* ¶ 40. We credit the testimony of Dr. Sears, who testifies that Bradford teaches a "player ID entry in a player ID database" in which the claimed biometric signature is stored and that "Yamane teaches using a presence/absence flag 60-2 to determine if a fingerprint has been registered." Ex. 1003 ¶¶ 61, 63 (citing Ex. 1006 ¶¶ 49, 52–54, 58–59, Fig. 2). Based on Bradford's "player ID database," the express disclosures of Yamane, and Dr. Sears' testimony, we are persuaded that Petitioner has shown a preponderance of evidence that Yamane in view of Bradford and Foss teaches limitation [1e].

(h) Motivation to combine Bradford and Yamane

Patent Owner also contends that Bradford and Yamane have "vast differences between [them]" and are improperly combined by Petitioner. PO Resp. 3–4, 23. Patent Owner submits that the "Petition ignores drastic differences between *Bradford* and *Yamane* that prove the only reason [Petitioner] has put these two references together is hindsight. *Id.* at 3–4. In particular, Patent Owner contends one of ordinary skill in the art "would not look to *Yamane* when seeking to modify the teaching of *Bradford*" because "*Yamane* teaches a 'rewritable area 1002' in which to store biometric information" which "is in direct contrast with the teachings of *Bradford*, which describe storing biometric information permanently." *Id.* at 23 (citing Ex. 1004, 23:36–40; Ex. 1006 ¶¶ 29, 31, 39, 41, Fig. 1; Ex. 2001 ¶ 60). Patent Owner also argues one of ordinary skill in the art would not seek to combine *Bradford* and *Yamane* because "*Bradford* is directed towards, in part, a casino machine, which is a stationary, single-purpose machine

typically designed to prevent any external interference" while "*Yamane* is directed towards a portable recording medium, namely a Compact Disc-Rewritable, a portable storage medium designed to be transported and read by different general-purpose computer machines." *Id.* (citing Ex. 1004, 32:66–33:14; Ex. 1006 ¶¶ 1, 10–12).

Petitioner's rationale underlying the obviousness of the combination of Bradford (with Foss) and Yamane does not rest on the permanency (or impermanency) of data storage, or on the mobility (or lack thereof) of a casino machine or compact disc-rewritable storage medium. Rather, Petitioner contends an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane because (i) "[t]here would have been a reasonable expectation of success in the proposed modification" that employs "[s]etting a flag . . . [which] is a well-known method of indicating a binary state," (ii) "[i]t would have required only routine programming to determine if the memory location comprising the second authenticator data field is occupied by setting the flag," and because (iii) "checking the value of a flag to determine if a biometric signature had been previously stored as taught by *Yamane*" would "provid[e] a fast and efficient method of completing the enrollment process taught by *Bradford*." Pet. 38–40; Pet. Reply 26–27.

Moreover, Patent Owner's distinction between Yamane's "*rewritable* area 1002" and Bradford's "data . . . read at the biometric reader . . . [being] permanently recorded into the field in the player ID datable" (*see* PO Resp. 23) is not persuasive because Yamane's area 1002-1 (where fingerprint registration presence/absence flags are recorded within rewritable area 1002) is "a protect area [of a data storage region]" in which "written data is

protected by encryption performed by a software." *See* Ex. 1006 ¶¶ 29, 31, 52, Fig. 1.

Patent Owner also contends "*Yamane* also teaches a CD-RW that is intended to transport multiple softwares to a wide variety of a terminals" which "cuts against any purported rationale to combine this reference with *Bradford*, which per the Petition teaches runs at most two software programs: a 'special, privileged screen used for demonstration purposes' and a 'standard, ready mode,' on a single type of machine (a gaming machine)." PO Resp. 24; *see also* PO Sur-Reply 12. Patent Owner further submits one of ordinary skill in the art would not seek to combine Bradford and Yamane because Bradford's storage mediums are either shared by connected casino machines or located on single casino machines, none therefore corresponding to "the portable storage medium taught by *Yamane*." PO Resp. 24.

Again, these arguments are unpersuasive because Petitioner's rationale underlying the obviousness of the combination of Bradford and Yamane is not based on the transportation (or lack thereof) of software to terminals, or on databases or storage mediums being highly portable. Rather, Petitioner contends an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane because

> [s]etting a flag in computer code is a well-known method of indicating a binary state. *Dec.*, 112. *Bradford* already teaches the hardware and software for storing the second authenticator data in the second authenticator data field. *Bradford*, 3:28–36. It would have required only routine programming to determine if the memory location comprising the second authenticator data field is occupied by setting the flag.

Pet. 38. Dr. Sears testifies that setting flags as taught by Yamane, and the reason for doing so, wereF well-known to those of ordinary skill in the art,

and that "[c]ombining *Yamane's* teachings with *Bradford* (as modified by *Foss*), would have required only routine programming to determine if the memory location that comprises the second authenticator data field is occupied (or not) by setting a flag." Ex. 1003 ¶ 112. Dr. Sears explains persuasively that setting a flag "would have reduced the required computing resources compared to having to actually read data stored in a referenced memory location and would have provided a fast and efficient method of completing *Bradford's* enrollment process." *Id.* Dr. Easttom does not agree that a person of ordinary skill in the art would have looked to Yamane, yet does not contradict Dr. Sears' description that using flags and the implementation of flags to indicate occupancy of a memory location were well-known to those of ordinary skill in the art for determining whether a memory location was unoccupied. *See* Ex. 2001 ¶¶ 57–62.

In the Sur-Reply, Patent Owner argues "*Bradford teaches away* from Yamane because [Bradford] describes the CD embodiment as '[c]learly not the optimal choice.'" PO Sur-Reply 12 (emphasis added) (citing Paper 13, 25). However, Bradford recognizes that CDs are a viable storage medium, and states that "each game device could be essentially a standalone machine if configured as shown in FIG. 3, with database updates being carried out by the use of CD-ROMs." Ex. 1004, 9:11–14. A reference does not teach away if it merely expresses a general preference for an alternative invention from amongst options available to the ordinarily skilled artisan, and the reference does not discredit or discourage investigation into the invention claimed. *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004); *see also In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006) ("A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led

in a direction divergent from the path that was taken by the applicant." (citations and internal quotation marks omitted)).

On the complete record now before us, we find that Petitioner and Dr. Sears have provided articulated reasoning with evidentiary underpinning as to why an ordinarily skilled artisan would have been motivated to combine the teachings of Bradford and Yamane. Pet. 37–40; Ex. 1003 ¶¶ 108–114.

(i) Conclusion as to claim 1

Based on the complete record before us and for the reasons expressed above, we are persuaded that Petitioner has shown a preponderance of evidence that claim 1 would have been obvious over Bradford, Foss, and Yamane.

5. Dependent Claim 2

Claim 2 depends from claim 1 and specifically recites "storing a biometric signature according to the enrolment method of claim 1." Ex. 1001, 12:41–42. Claim 2 specifically recites "[a] method of securing a process at a verification station." *Id.* at 12:39. Thus, different from the enrollment process of claim 1, claim 2 is directed to a verification process that follows the enrollment process.

Patent Owner does not provide substantive arguments with respect to claim 2, mainly arguing that claim 2 contains the same method steps of claim 1 and "[a]s the prior art cited by [Petitioner] does not teach these limitations, the cited prior art does not render these dependent claims obvious as a result thereof." PO Resp. 25.

Petitioner argues that Bradford's system "is used for securing and obtaining verified access to a game device or authenticating a user." Pet. 41 (citing Ex. 1002 ¶¶ 115–116). And, as described above, Petitioner also

argues that "*Bradford* teaches storing a biometric signature (*Bradford*, 15:60–63, FIG. 6), and the *Bradford-Foss-Yamane* combination teaches the enrollment method of Claim 1." *Id.*

> Claim 2 recites in pertinent part the additional step of:
>
> verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

Ex. 1001, 12:45–50. Petitioner argues that Bradford describes a verification process that verifies the card information of a player when "[t]he player then goes and uses a game device. . . [t]he player presents their first authenticator to the game device. Pet. 42 (quoting Ex. 1004, 13:23–33). Petitioner next contends that, as described for limitations [1c]–[1e], and as for a second authenticator, "the *Bradford-Foss-Yamane* system teaches storing a biometric signature at a location in local memory defined by card information." *Id.* at 43. Petitioner argues that

> *Bradford* teaches that, subsequent to verification of the presented card information required to perform a transaction (such as transfer funds, authorize a form, or play a game), "the second authenticator is checked, and **if the fingerprint data just read matches the fingerprint data in the second authenticator**, the action is **authorized** and carried out."

Id. at 43–44 (quoting Ex. 1004, 3:66–4:2). Dr. Sears testifies that in Bradford's gaming device 300 "if the first authenticator is verified (i.e., determined to be valid), then the steps for verifying the second authenticator data (for example, a fingerprint) occur." Ex. 1003 ¶ 118 (citing Ex. 1004, 3:50–62, 13:23–33, 17:14–27, 17:47–51, 18:27–39, 24:52–25:25).

Petitioner's arguments and Dr. Sears' testimony are consistent with Bradford's disclosure. For example, Bradford expressly describes a

verification procedure using a first and second authenticator, where the second authenticator is a biometric signature, i.e., a fingerprint:

> The player presents their first authenticator to the game device, which is used to get the associated second authenticator . . . [r]emembering that the second authenticator is always biometric data, all the player has to do is use the biometric reader. In the case of fingerprints, a quick touch of a fingerprint reader does the job. The second authenticator is checked, and if the fingerprint data just read matches the fingerprint data in the second authenticator, the action is authorized and carried out.

Ex. 1004, 3:50–4:2

For dependent claim 2 we have considered and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 41–42 of the Petition. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claim 2 would have been obvious over Bradford, Foss, and Yamane.

6. Claims 19 and 20

Independent claim 19 and dependent claim 20 include essentially the same limitations as claims 1 and 2, except, that the preamble to claim 19 recites:

> A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

Ex. 1001, 15:25–16:2. And, for example, the limitation of "receiving card information," in independent claim 1, is recited in independent claim 19 as "code for receiving card information."

Petitioner argues that a person of ordinary skill in the art "would have understood *Bradford* teaches the game device 300 of FIG. 3 includes at least one processor, memory, and software for performing the disclosed functions

for game device 300." Pet. 44 (citing Ex. 1003 ¶¶ 122–124). Dr. Sears testifies that "a POSITA would have understood that *Bradford* teaches that the game device 300 (depicted in Fig. 3) includes a central processor, associated memory, firmware, software, and the other 'normal and well known internals' as taught by *Bradford*." Ex. 1003 ¶ 123. Dr. Sears explains that a person of ordinary skill in the art "would have understood and found obvious that processors execute programming instructions (e.g., software) to perform various functions." *Id.* ¶ 124. In addition, Dr. Sears explains that a skilled artisan "would have understood that *Bradford's* software would have been stored in non-transitory memory for several reasons, including so that the game device would still be functional even if powered off and on again (i.e., power cycled)." *Id.* ¶ 126. Dr. Sears' testimony as to what a person of ordinary skill in the art would understand in regards to the known internals, programming instructions, and memory structure for a game device as shown in Bradford's Figure 3 is unrebutted on this record.

Petitioner's arguments and evidence are in all other respects the same as the arguments and evidence presented with respect to claims 1 and 2. We have considered, and on the complete record before us, accept as our own, Petitioner's arguments and evidence set forth at pages 44–48 of the Petition as to claims 19 and 20. Accordingly, we determine that Petitioner has shown by a preponderance of the evidence that claims 19 and 20 would have been obvious over Bradford, Foss, and Yamane for the same reasons as claims 1 and 2.

III. CONCLUSION[12]

For the reasons discussed above, we determine Petitioner has met its burden of establishing by a preponderance of the evidence that the challenged claims are unpatentable as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 2, 19, 20	103	Bradford, Foss, Yamane	1, 2, 19, 20	
Overall Outcome			1, 2, 19, 20	

IV. ORDER

For the reasons given, it is

ORDERED that, based on a preponderance of the evidence, claims 1, 2, 19, and 20 of the '039 patent have been shown to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, any party to the proceeding seeking judicial review of this Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

[12] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

For PETITIONER:

Jennifer C. Bailey
Adam P. Seitz
ERISE IP, P.A.
PTAB@eriseip.com
jennifer.bailey@eriseip.com
adam.seitz@eriseip.com

PATENT OWNER:

Darlene F. Ghavimi-Alagha
Brian P. Bozzo
K&L Gates LLP
darlene.ghavimi@klgates.com
brian.bozzo@klgates.com

US008620039B2

(12) **United States Patent**
Burke

(10) **Patent No.: US 8,620,039 B2**
(45) **Date of Patent: Dec. 31, 2013**

(54) **CARD DEVICE SECURITY USING BIOMETRICS**

(75) Inventor: **Christopher John Burke**, Ramsgate (AU)

(73) Assignee: **Securicom (NSW) Pty Ltd**, New South Wales (AU)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 912 days.

(21) Appl. No.: **12/063,650**

(22) PCT Filed: **Aug. 10, 2006**

(86) PCT No.: **PCT/AU2006/001136**

§ 371 (c)(1),
(2), (4) Date: **Aug. 12, 2010**

(87) PCT Pub. No.: **WO2007/019605**

PCT Pub. Date: **Feb. 22, 2007**

(65) **Prior Publication Data**

US 2010/0296708 A1 Nov. 25, 2010

(30) **Foreign Application Priority Data**

Aug. 12, 2005 (AU) 2005904375

(51) **Int. Cl.**
G06K 9/00 (2006.01)

(52) **U.S. Cl.**
USPC **382/119**; 340/5.82

(58) **Field of Classification Search**
USPC 382/115, 119, 155, 159; 356/71; 350/5.2, 5.52, 5.53, 5.8, 5.81, 5.82, 350/5.83; 235/380, 382; 340/5.2, 5.52, 340/5.53, 5.8, 5.81, 5.82, 5.83
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,457,747	A	10/1995	Drexler et al.	380/24
6,665,601	B1	12/2003	Nielsen	701/50
6,796,492	B1	9/2004	Gatto	235/379
2004/0041690	A1	3/2004	Yamagishi	340/5

FOREIGN PATENT DOCUMENTS

CA	2 412 403	A1	5/2003
WO	WO 03/036861	A1	5/2003
WO	WO 2004/100053	A1	11/2004

OTHER PUBLICATIONS

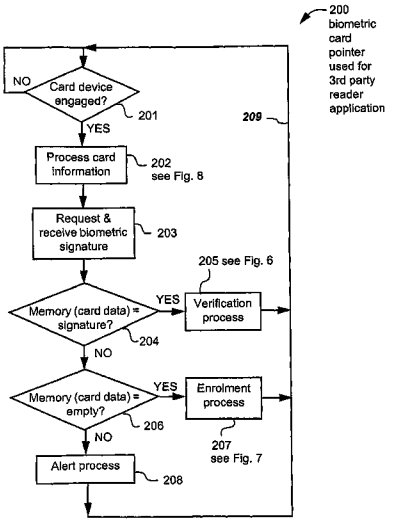
International Search Report dated Oct. 20, 2006.
International Preliminary Report on Patentability dated Nov. 19, 2007.
Supplementary European Search Report dated Aug. 29, 2011 for EPO Application No. EP 06760981.8.

Primary Examiner — Andrew W Johns
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

The disclosed Biometric Card Pointer arrangements store (**207**) a card user's biometric signature in a local memory (**124**) in a verification station (**127**) the first time the card user uses the verification station (**127**) in question. The biometric signature is stored at a memory address (**607**) defined by the card information (**605**) on the user's card (**601**). All future uses of the particular verification station (**127**) by someone submitting the aforementioned card (**601**) requires the card user to submit both the card and a biometric signature, which is verified against the signature stored at the memory address defined by the card information (**605**) thereby determining if the person submitting the card is authorized to do so.

20 Claims, 7 Drawing Sheets



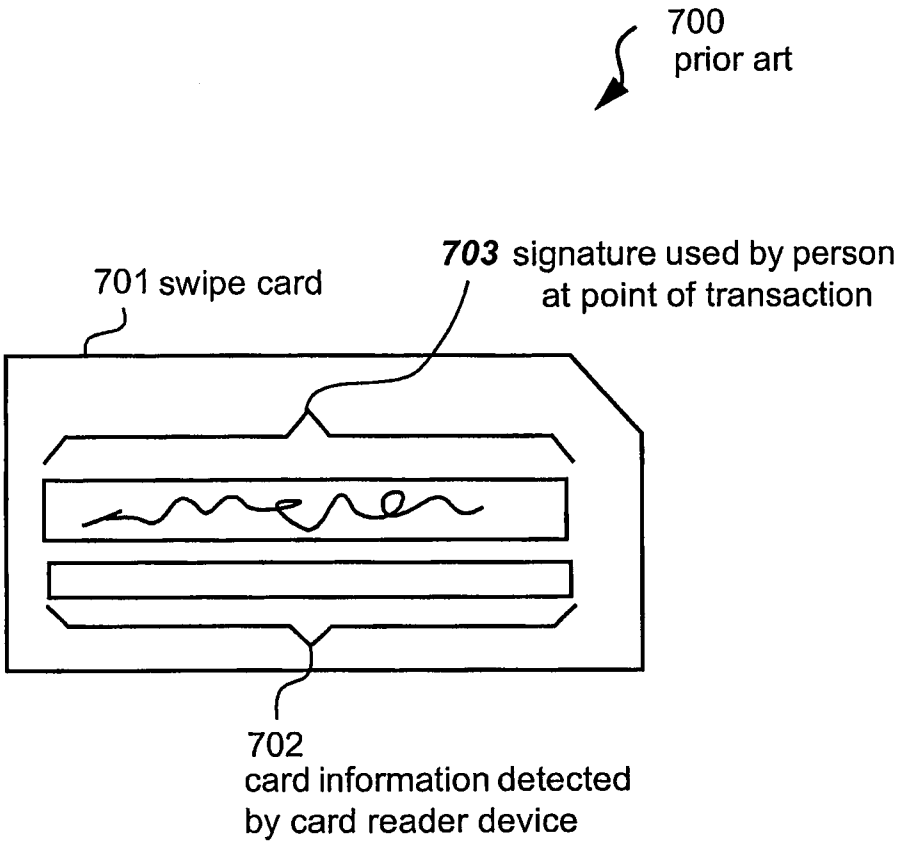


Fig. 1
prior art

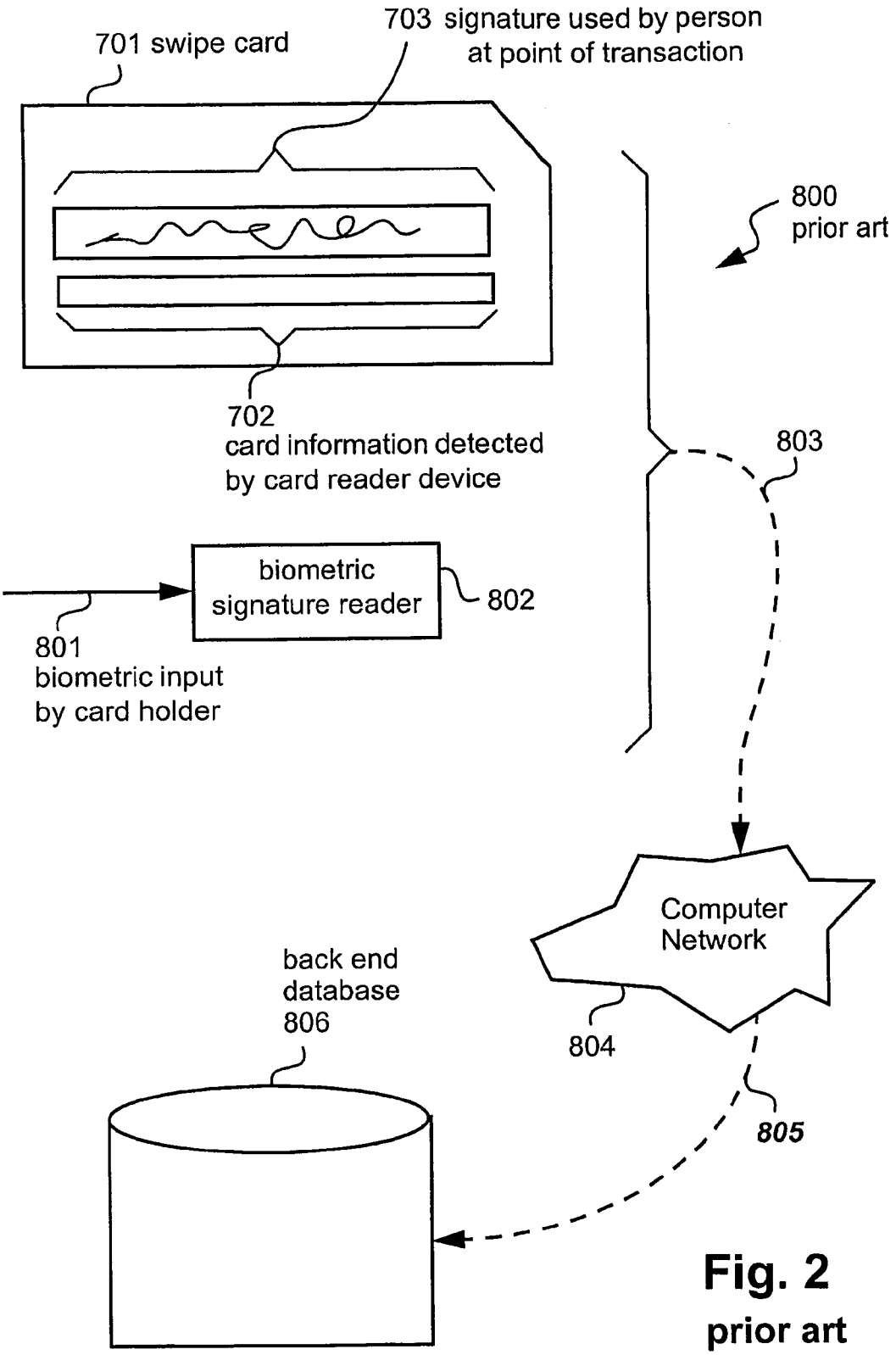


Fig. 2
prior art

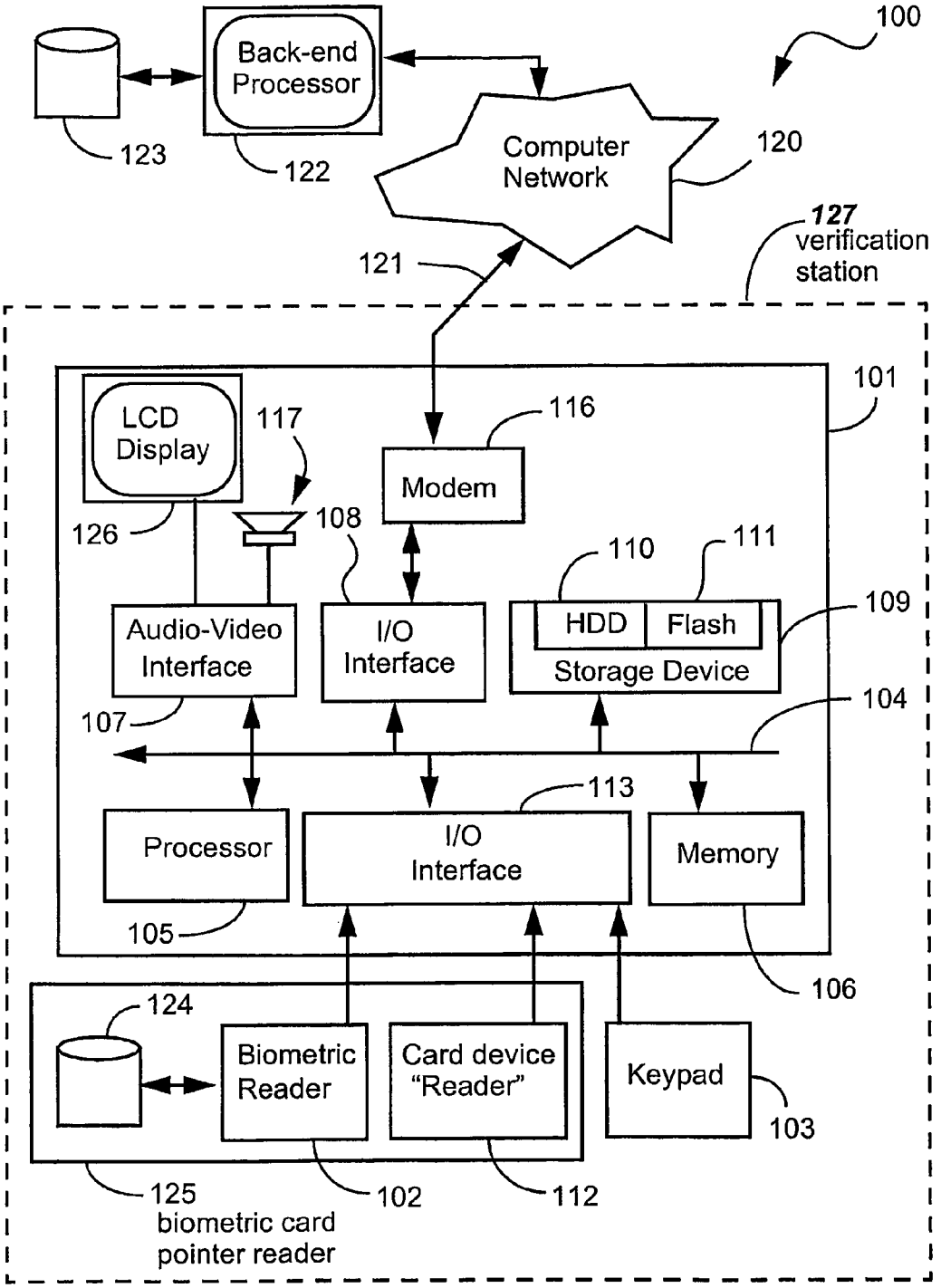

100
Back-end Processor
123
122
Computer Network
120
127 verification station
121
101
LCD Display
117
116
Modem
126
108
110
111
Audio-Video Interface
I/O Interface
HDD
Flash
Storage Device
109
107
104
113
Processor
I/O Interface
Memory
105
106
124
Biometric Reader
Card device "Reader"
Keypad
103
125 biometric card pointer reader
102
112

Fig. 3

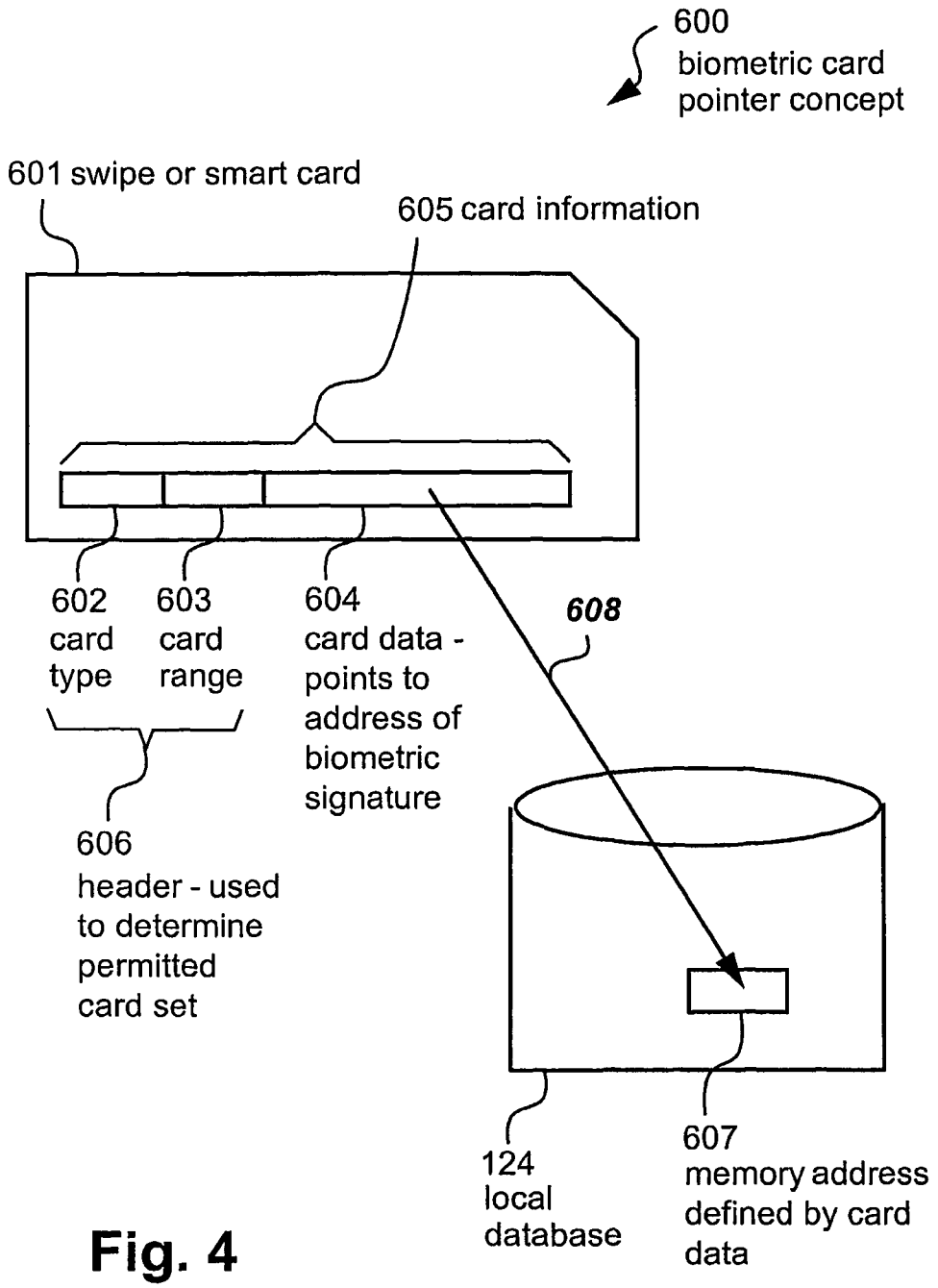

600
biometric card
pointer concept
601 swipe or smart card
605 card information
602
card
type
603
card
range
604
card data -
points to
address of
biometric
signature
608
606
header - used
to determine
permitted
card set
124
local
database
607
memory address
defined by card
data

Fig. 4

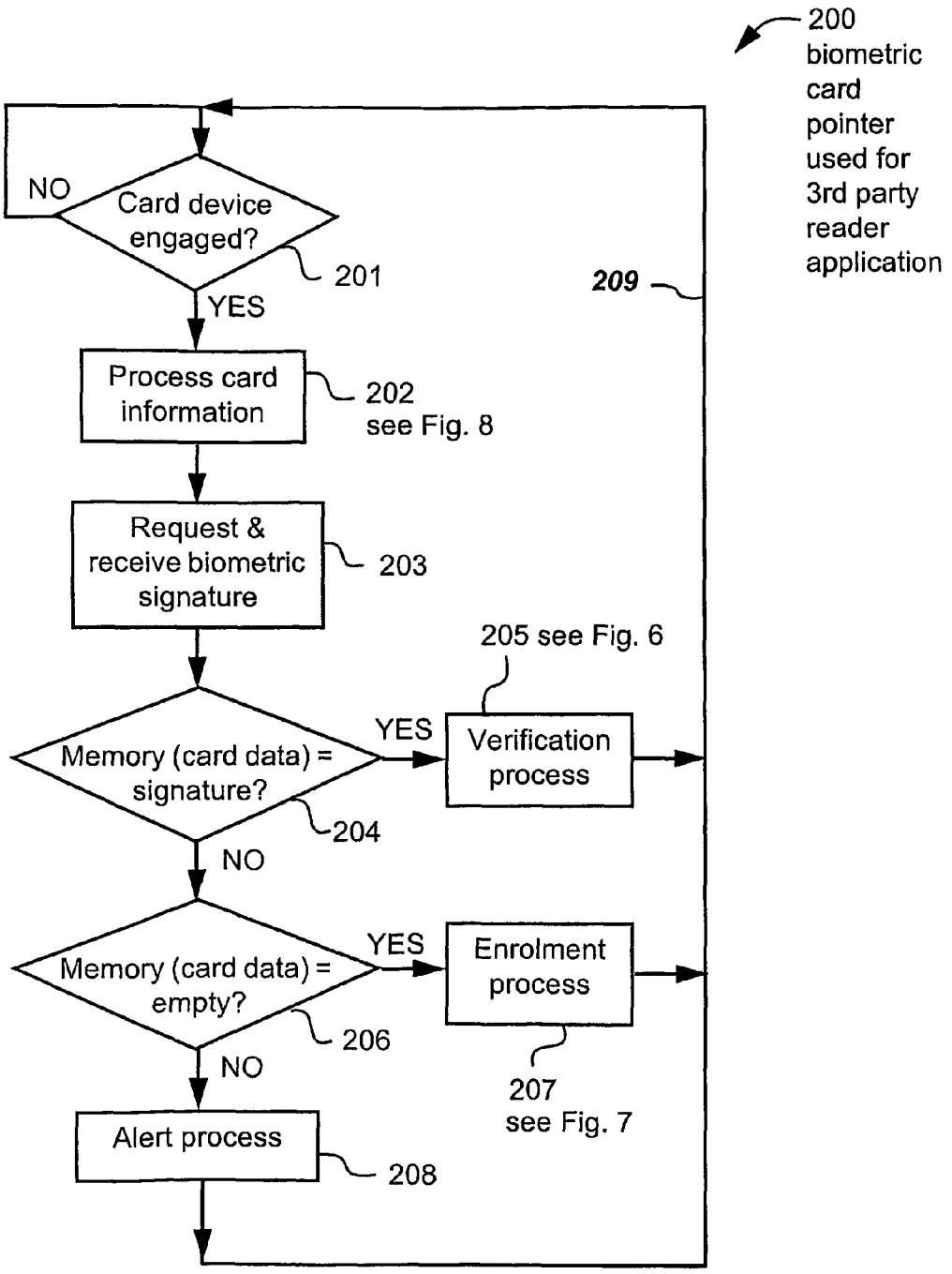

200
biometric
card
pointer
used for
3rd party
reader
application
Card device engaged?
NO
YES
201
209
Process card information
202
see Fig. 8
Request & receive biometric signature
203
205 see Fig. 6
Memory (card data) = signature?
YES
Verification process
204
NO
Memory (card data) = empty?
YES
Enrolment process
206
NO
207
see Fig. 7
Alert process
208

Fig. 5

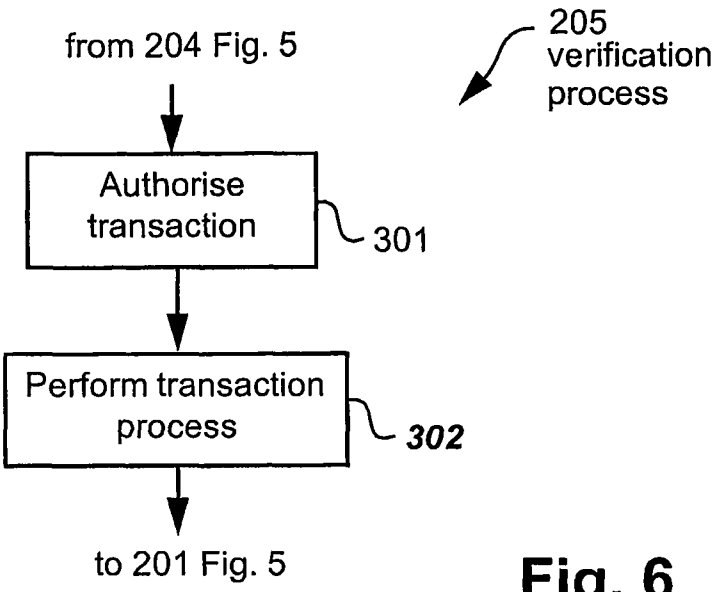

from 204 Fig. 5
205
verification
process
Authorise
transaction
301
Perform transaction
process
302
to 201 Fig. 5

Fig. 6

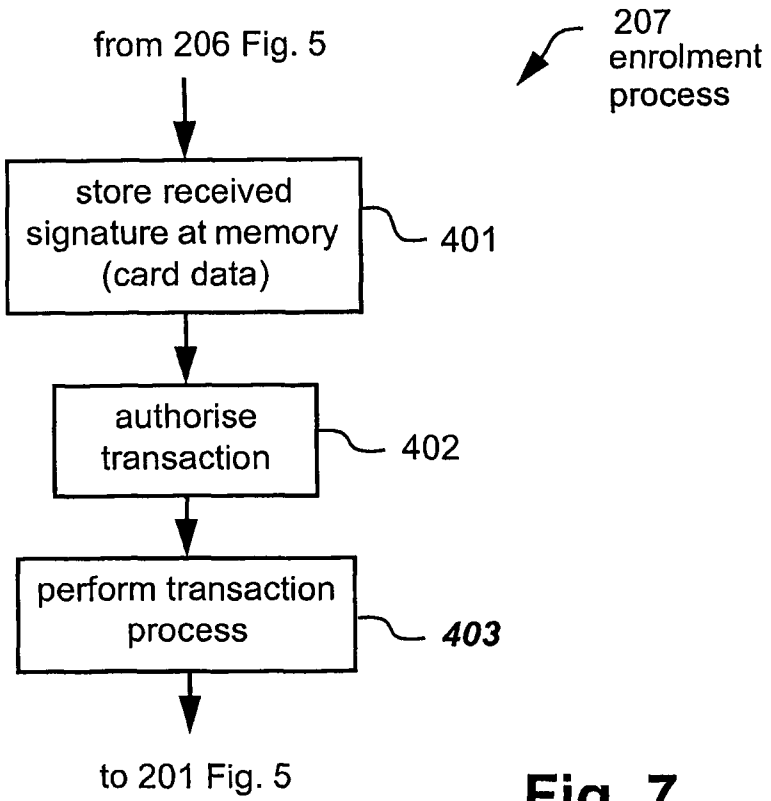

from 206 Fig. 5
207
enrolment
process
store received
signature at memory
(card data)
401
authorise
transaction
402
perform transaction
process
403
to 201 Fig. 5

Fig. 7

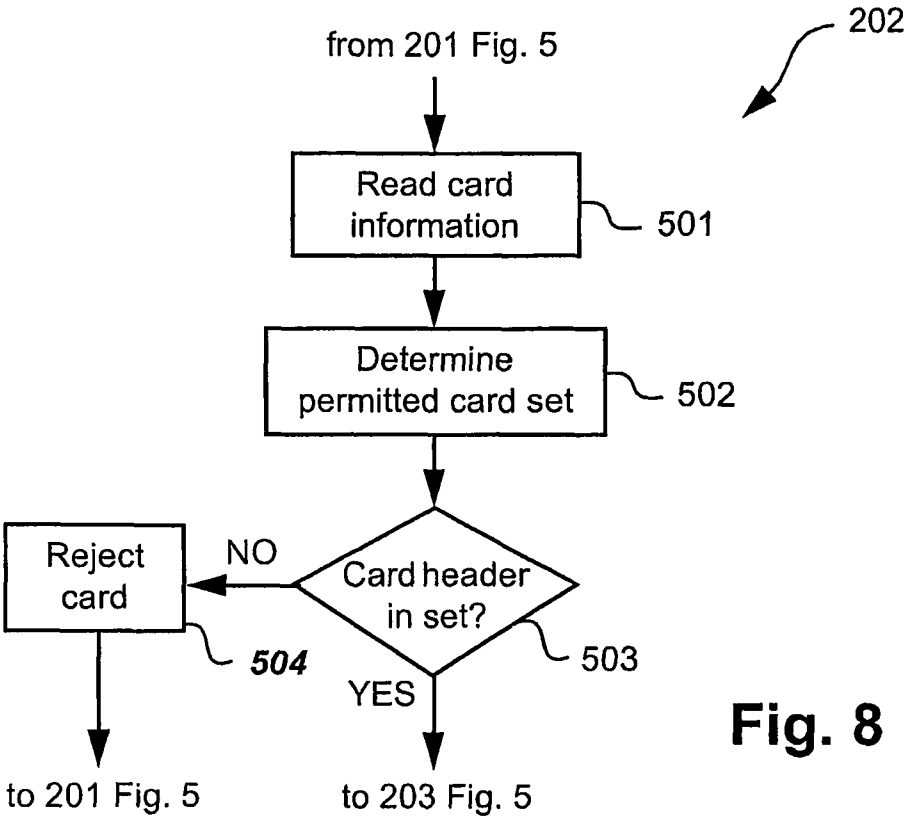

from 201 Fig. 5
202
Read card information
501
Determine permitted card set
502
Card header in set?
503
NO
Reject card
504
YES
to 201 Fig. 5
to 203 Fig. 5

Fig. 8

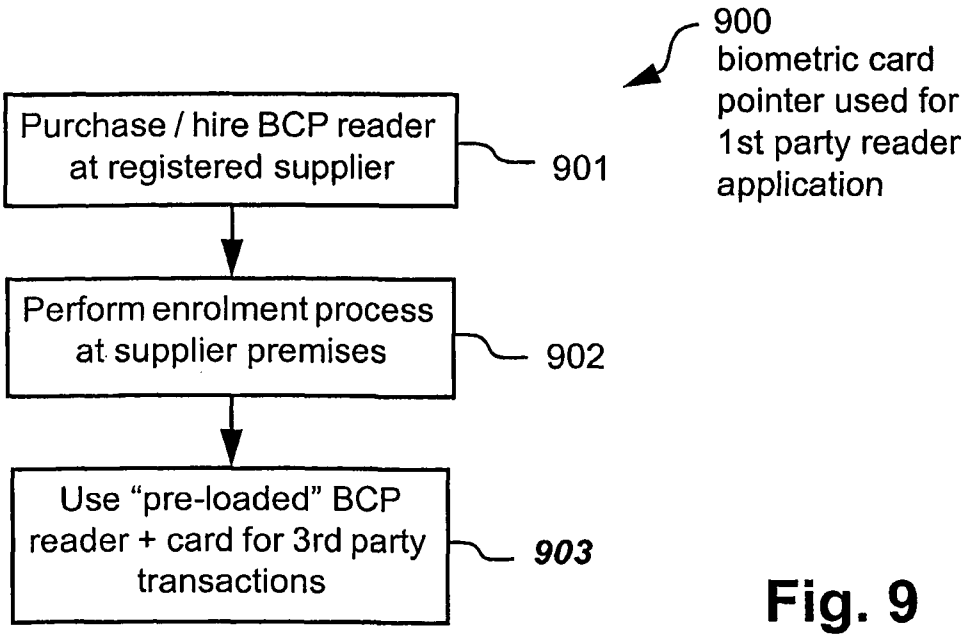

900
biometric card pointer used for 1st party reader application
Purchase / hire BCP reader at registered supplier
901
Perform enrolment process at supplier premises
902
Use "pre-loaded" BCP reader + card for 3rd party transactions
903

Fig. 9

CARD DEVICE SECURITY USING BIOMETRICS

This application is the National Stage of International Application No. PCT/AU2006/001136, filed Aug. 10, 2006, which claims the benefit of priority to Australian Patent Application No. 2005904375, filed on Aug. 12, 2005. All of the foregoing applications are hereby incorporated herein in their entirety in this application.

FIELD OF THE INVENTION

The present invention relates generally to security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.

BACKGROUND

This description makes reference to various types of "card device" and their associated "reader devices" (respectively referred to merely as cards and readers). The card devices all contain card information that is accessed by "coupling" the card device to an associated reader device. The card information is used for various secure access purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account and so on. The card information is typically accessed from the card by a corresponding card reader which then sends the card information to a "back-end" system that completes the appropriate transaction or process.

One type of card is the "standard credit card" which in this description refers to a traditional plastic card **701** as depicted in FIG. **1**. The standard credit card is typically "swiped" through a slot in a standard credit card reader in order to access card information **702** on the card **701**. The card information **702** can alternately be encoded using an optical code such as a bar code, in which case the reader is suitably adapted. The standard credit card **701** also typically has the signature **703** of the card-owner written onto a paper strip on the card **701**. This is used for verification of the identity of the person submitting the card when conducting a transaction using the card **701**.

Another type of card device is the smart card (not shown) that typically has an on-board processor and a memory. The smart card typically has electrical contacts that mate with corresponding contacts on a smart card reader (not shown) when accessing data in the memory of the smart card.

Another type of card device is the wireless "key-fob" which is a small radio transmitter that emits a radio frequency (RF) signal when a button on the fob is pressed. The RF signal can be encoded using the Wiegand protocol, or any other suitable protocol, such as rolling code or Bluetooth™ and can include encryption if desired. The key-fob typically has a processor and memory storing data that is sent via the transmitted signal to a corresponding receiver, which is the "reader device" for this type of card device.

The description also refers to "card user" and "card owner". The card user is the person who submits the card for a particular transaction. The card user can thus be the (authorised) card owner or an (unauthorised) person who has found or stolen the card.

Clearly the signature **703** on the standard credit card **701** in FIG. **1** can be forged. Thus, if the standard card **701** is stolen or lost, an unauthorised user can use the card provided that they can supply a sufficiently accurate version of the signature

703. The only recourse available to the card owner is to notify the card issuing company to "cancel" the card.

Current card devices such as the standard credit card, the smart card and the key-fob can have their security enhanced by requiring the card user to provide PIN (Personal Identification Number) information through a keypad to verify their identity prior to completing a transaction. However, PIN information can also be "stolen" by surveillance of the card owner's hands as the card owner operates the keypad.

Biometric verification can also be incorporated into current card systems to enhance security. In FIG. **2** the card user swipes the standard card **701** through an associated card reader (not shown) that accesses the card information **702** on the card **701**. The card user also provides a biometric input **801**, for example by pressing their thumb against a biometric (eg fingerprint) reader **802**. The card information **702** that is read by the card reader (not shown), together with the biometric signature that is read by the biometric (fingerprint) reader **802**, are sent, as depicted by a dashed arrow **803**, a computer network **804**, and a further dashed arrow **805**, to a back-end system including a database **806** and associated processor (not shown).

In this arrangement, the card owner needs to have previously registered their biometric signature **801** and the card information **702** for pre-loading onto the back-end database **806**. Having done so, the back-end processor (not shown) compares the pre-loaded information on the database **806** with the information received at **805**, in order to check that the card holder of the card **701** is the (authorised) card owner and that the card itself is valid, in which case the transaction in question can proceed. Clearly this arrangement requires a central repository (**806**) of card information **702** and biometric information **801**. This is cumbersome and potentially compromises the privacy of the holder of the card **701**. This arrangement also requires complex back-end database management and the communications network **804**. Furthermore, the front-end biometric signature reader **802** requires storage and/or processing capabilities for the biometric signatures. This results in a complex and expensive solution.

Privacy concerns have also been raised against the arrangement of FIG. **2** which involves centralised storage and processing of personal information including biometric information. These concerns have slowed widespread use of biometrics to enhance user verification.

SUMMARY

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

Disclosed are arrangements, referred to as Biometric Card Pointer (BCP) arrangements or systems, which seek to address the above problems relating to secure access and/or secure processes, by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, a biometric signature reader, the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form), an alphanumeric keypad (optional), and a communication module for communicating with back-end system that may be remotely accessible over a network.

The card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase). The biometric signature is stored at a memory address defined by the ("unique") card information on the user's card as read by the card reader of the verification station. Clearly the term

"unique" means unique in the context of a permitted set of cards associated with the verification station. This is described in more detail in regard to FIG. **8**.

All future uses (referred to as uses in the verification phase) of the particular verification station by someone submitting the aforementioned card requires the card user to submit both the card to the card reader and a biometric signature to the biometric reader, which is verified against the signature stored at the memory address defined by the card information thereby determining if the person submitting the card is authorised to do so.

Each use of the verification station is identical from the card user's perspective, requiring merely input of the card to the card reader, and provision of the biometric signature (eg thumb print or retinal scan etc.) to the biometric reader.

An authorised card user will be automatically verified by the BCP arrangement in the verification station, and the corresponding transaction, be it an ATM cash withdrawal, a credit purchase, a loyalty point update etc. will simply proceed as normal. An unauthorised card user (ie a card user who misappropriated the card after the initial enrolment) will not receive authorisation, and the intended transaction will not proceed. Furthermore, the biometric signature of the unauthorised user will be captured in the verification station, and can be used by the authorities to track the unauthorised user and prove misappropriation of the card.

The disclosed BCP arrangements require little if any modification of the back-end systems or the (front-end) card. The additional administrative overheads associated with the BCP arrangements, above those already required for systems using (standard) cards and back-end systems, are minimal. The BCP arrangements also potentially have a reduced impact on privacy of card users. The biometric signatures stored in the local database of the verification station can be made off limits to anyone, or limited to law enforcement agencies, depending on the administrative environment in which the BCP arrangements are implemented. Users of current card systems can learn to use BCP arrangements without much effort, needing only to provide a biometric signature when asked to do so at the verification station. The difference between the enrolment and verification phases are transparent to users, further reducing the effort in learning how to use the BCP arrangements.

According to a first aspect of the present invention, there is provided a method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature; and

storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to another aspect of the present invention, there is provided a method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the noted enrolment method;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

According to another aspect of the present invention, there is provided a method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to another aspect of the present invention, there is provided a verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for;

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to another aspect of the present invention, there is provided a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for;

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for;

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

According to another aspect of the present invention, there is provided a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature; and

code for storing, if a memory location defined by the card information is unoccupied, the biometric signature at the defined memory location.

According to another aspect of the present invention, there is provided a computer program product including a computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the noted enrolment method;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location defined by the subsequently presented card information.

Other aspects of the invention are also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

Some aspects of the prior art and one or more embodiments of the present invention will now be described with reference to the drawings, in which:

FIG. **1** depicts a standard credit card;

FIG. **2** shows the card of FIG. **1** being used together with biometric verification;

FIG. **3** is a functional block diagram of a special-purpose computer system upon which described methods for the BCP arrangements can be practiced;

FIG. **4** illustrates the biometric card pointer concept;

FIG. **5** is a flow chart of a process for using the biometric card pointer arrangement;

FIG. **6** shows the verification process of FIG. **5** in more detail;

FIG. **7** shows the enrolment process of FIG. **5** in more detail;

FIG. **8** shows the card information process of FIG. **5** in more detail; and

FIG. **9** shows an alternate use for the biometric card pointer arrangement.

DETAILED DESCRIPTION INCLUDING BEST MODE

Where reference is made in any one or more of the accompanying drawings to steps and/or features, which have the same reference numerals, those steps and/or features have for the purposes of this description the same function(s) or operation(s), unless the contrary intention appears.

FIG. **3** is a functional block diagram of a system **100** in which the disclosed BCP arrangements can be practiced. The disclosed BCP methods particularly lend themselves to implementation on the special-purpose computer system **100** such as that shown in FIG. **3** wherein the processes of FIGS. **5-8** and **9** may be implemented as software, such as a BCP application program executing within the computer system **100**. In particular, the steps of the BCP processes are effected by instructions in the BCP software that are carried out by a verification station **127**. The verification station **127** is typically constructed in a tamper-proof manner, both physically and electronically, to prevent unauthorised access to the inner mechanism of the verification station **127**. The instructions may be formed as one or more code modules, each for performing one or more particular tasks. The BCP software may also be divided into two separate parts, in which a first part performs the BCP methods and a second part manages a user interface between the first part and the user.

The BCP software may be stored in a computer readable medium, including the storage devices described below, for example. The BCP software is loaded into the verification station **127** from the computer readable medium, and then executed by the verification station **127**. A computer readable medium having such software or computer program recorded on it is a computer program product. The use of the computer program product in the computer preferably effects an advantageous apparatus for effecting the BCP arrangements.

The verification station **127** comprises, in the described arrangement, a biometric card pointer reader **125**, a keypad **103**, and a computer module **101**. The biometric card pointer reader is made up of a biometric reader **102**, a card device reader **112** and a local database **124**.

The computer system **100** consists of a computer module **101**, input devices such as a biometric reader **102**, a card reader **112**, and a keypad **103**, output devices including an LCD (Liquid Crystal Display) display device **126** and a loudspeaker **117**. The computer module **101** uses a Modulator-Demodulator (Modem) transceiver device **116** for communicating to and from a communications network **120**, for example connectable via a telephone line **121** or other functional medium. The modem **116** can be used to obtain access to a back end system including a processor **122** and back-end database **123** over the Internet, and other network systems, such as a Local Area Network (LAN) or a Wide Area Network (WAN).

The computer module **101** typically includes at least one processor unit **105**, and a memory unit **106**, for example formed from semiconductor random access memory (RAM) and read only memory (ROM). The module **101** also includes a number of input/output (I/O) interfaces including an audio-video interface **107** that couples to the LCD display **126** and loudspeaker **117**, an I/O interface **113** for the keypad **103**, biometric reader **102** and card reader **112**, and an interface **108** for the modem **116**. In some implementations, the modem **1116** may be incorporated within the computer module **101**, for example within the interface **108**.

A storage device **109** is provided and typically includes a hard disk drive **110** and a flash memory **111**. The components **105**, to **111** and **113** of the computer module **101**, typically communicate via an interconnected bus **104** and in a manner that results in a conventional mode of operation of the computer system **100** known to those in the relevant art.

Typically, the BCP application program is resident on the hard disk drive **110** and read and controlled in its execution by

the processor **105**. Intermediate storage of the program and any data fetched from the network **120** may be accomplished using the semiconductor memory **106**, possibly in concert with the hard disk drive **110**. In some instances, the BCP application program may be supplied to the user encoded on the flash memory device **111**, or alternatively may be read by the computer module **101** from the network **120** via the modem device **116**.

Still further, the software can also be loaded into the computer system **100** from other computer readable media. The term "computer readable medium" as used herein refers to any storage or transmission medium that participates in providing instructions and/or data to the computer system **100** for execution and/or processing. Examples of storage media include floppy disks, magnetic tape, CD-ROM, a hard disk drive, a ROM or integrated circuit, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computer module **101**. Examples of transmission media include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

As illustrated in FIG. **4**, a standard card **601** has card information **605** typically comprising three fields, namely **602** which is the card type, **603** which is the card range, and **604** which comprises card data specific to the particular card **601**. The card information **605** can be encoded using a magnetic strip, a bar code, or a solid state memory on the card **601**. Alternately, the card device can be implemented as a wireless key fob. In one example of the disclosed BCP approach, the card data **604** acts as the memory reference which points, as depicted by an arrow **608**, to a particular memory location at an address **607** in the local database **124** in the verification station **127** of FIG. **3**. The fields **602** and **603**, which together form a header **606**, can be used by the disclosed BCP system to determine if the card **601** is to be processed according to the disclosed BCP approach or not. This is described in more detail in regard to FIG. **8**. Alternately, any segment of the card information **605** can be used as the memory reference which points to the particular memory location in the local database **124**.

In an initial enrolment phase, the card user couples their card **601** (or key-fob or other card device) to the card reader **112**. The card user is then required to input a biometric signature, such as fingerprint, face, iris, or other unique signature, into the biometric reader **102**. The card data **604** defines the location **607** in the memory **124** where their unique biometric signature is stored.

Thereafter, in later verification phases, the user couples their card **601** to the card reader **112**, after which the card user is required to again present their unique biometric to the biometric reader **102**. This signature is compared to the signature stored at the memory location **607** in the memory **124**, the memory location **607** being defined by the card data **604** read from their card **601** by the card reader **112**. Once verification is confirmed, the card information **605** is transferred from the verification station **127** to the back-end processor **122** for completion of the transaction.

Importantly, the back-end processor **122** does not see the difference between receiving the card information **605** from the verification station **127**, and receiving it from a conventional card reader in the absence of the verification station implementing the disclosed BCP arrangement. This means that back-end processes (depicted by the back-end processor **122** and the back-end database **123**) need no modification when incorporating the BCP arrangement into current card systems. There are additional elements in the verification station **127** (see FIG. **3**) compared to the normal card reader, however this is a relatively simple an inexpensive upgrade compared to the centralised arrangement depicted in FIG. **2**.

FIG. **5** shows a process **200** for normal use of the BCP approach. In a first step **201**, the processor **105** determines if the card **601** has been read by the card reader **112**. If this is not the case, then the process **200** follows a NO arrow back to the step **201**. If, on the other hand, the card **601** has been read by the card reader **112**, then the process **200** follows a YES arrow to a step **202** (see FIG. **8** for more details). In the step **202**, the processor **105** processes the card information **605** that is read from the card **601** by the card reader **112**. In a following step **203** a request is presented to the card holder to provide a biometric signature to the biometric reader **102**. This request can be provided in an audio fashion by means of the audio interface **107** and the speaker **117**, this being driven by suitable software running on the processor **105**. Alternatively or in addition, a suitable message can be displayed on the LCD display **126** by suitable software running on the processor **105**.

In response to the aforementioned request, the holder of the card **601** provides a biometric signature to the biometric reader **102**. After the signature has been received by the step **203**, the process **200** is directed to a step **204** that reads the contents of the local database **124** at an address defined by the card data **604**. If the contents of this memory address match, to a sufficiently high degree of correspondence, the biometric signature received in the step **203** via the biometric reader **102**, then the process follows a YES arrow to a step **205** (see FIG. **6** for more detail). It is noted that if the step **204** returns a YES value, then the biometric signature at the noted memory address was written into the memory **124** in an earlier enrolment phase. It is also noted that the step **204** reads the contents stored at a single memory address defined by the card data **604** and checks these contents against the biometric signature received in the step **203**. There is no need to search the entire database **124** to see if there is a match. Thus the disclosed BCP arrangement provides a particularly simple and fast biometric verification check thereby securing the process associated with the step **205**. Once the step **205** has completed the verification process, the process **200** is directed according to an arrow **209** back to the step **201**.

In an alternate arrangement, the card data **604** can be associated with a group of memory locations, rather than being the address for a specific memory location. This arrangement allows a different biometric signature to be stored in each of the group of memory locations, and in this case, the step **204** reads the contents stored in each memory location in the group defined by the card data **604**, and checks the contents of each memory location in the group against the biometric signature received in the step **203**. If the contents of any member of the group of memory locations matches, to a sufficiently high degree of correspondence, the biometric signature received in the step **203** via the biometric reader **102**, then the process follows a YES arrow to a step **205**. This arrangement allows, for example, two cards having the same card data **604** to be used at the same verification station **127** after each card holder performs their own individual enrolment process.

Returning to the step **204**, if the contents of the local database **124** at the memory address defined by the card data **604** does not match the signature received by the biometric reader **102**, then the process **200** follows NO arrow to a step **206**. In the step **206**, the processor **105** determines if the contents of the memory defined by the card data **604** is empty. If this is the case, then the process **200** follows a YES arrow to

a step **207** that performs an enrolment process for the card **601** (see FIG. **7** for more detail). The process **200** then follows the arrow **209** back to the step **201**.

Returning to the step **206**, if the contents of the aforementioned memory location is not empty, then this means that (i) the card **601** and the associated biometric signature of the card holder have previously been used for the enrolment process **207**, and (ii) the biometric signature now received in the step **203** does not match the signature stored in the database **124**. In this event, the process **200** follows a NO arrow to a step **208** that performs an alert process. The process **200** then follows the arrow **209** back to the step **201**. The alert process **208** can include sending an alert message from the verification station **127** to the back end processor **122** for later action, for example by the police. The alert process can also store the (unauthorised) signature for later use by the law enforcement authorities, and can capture the card in the verification station **127**, thereby removing the card from the possession of the apparently unauthorised person.

The alert process **208** can send, as part of the alert message, send all or part of the card information **605** that is input to the verification station **127** in the step **201** of FIG. **5**.

Although in the above description the step **206** tests if the memory location defined by the card data **604** is "empty", other approaches can be used. Thus when enrolment is performed, resulting in a memory location being used to store a biometric signature (eg see step **401** in FIG. **7**), a flag can be set to indicate that the memory location in question is occupied. The term "occupied" in this context means that the memory location in question has been used in the enrolment process for a user, and that the information stored at the memory location in question has not been deleted by a BCP system administrator. If the signature stored in the database **124** at the particular memory location is deleted by a BCP system administrator (as described in regard to FIG. **8**) then the flag can be reset to indicate that the memory location in question is no longer occupied.

As noted in regard to FIG. **3**, the verification station **127** is constructed in a tamper proof fashion to ensure that the process **200** of FIG. **5**, particularly the steps **204-207**, are not accessible to unauthorised tampering.

FIG. **6** shows the verification process **205** from FIG. **5** in more detail. The process **205** is entered from the step **204** in FIG. **5**, after which a step **301** authorises the transaction. This authorisation step **301** indicates that the biometric signal received by the biometric reader **102** in the step **203** matches the biometric signature previously stored in the local database **124** by a previous enrolment process **207** applied to the card in question.

After the step **301**, a step **302** performs the transaction process (which may be viewed as a process of obtaining verified access to a protected resource), whatever that may be. Thus, for example, if the process **200** of FIG. **5** relates withdrawal of cash from an Automatic Teller Machine (ATM) operated by one of a number of service providers, then the step **302** comprises the user specifying the required amount of cash and the relevant account information via the keypad **103** (see FIG. **3**), and the provision of a receipt and cash by the ATM (not shown). After completion of the transaction process by to the step **302**, the process **205** is directed back to the step **201** in FIG. **5**.

FIG. **7** shows the enrolment process step **207** from FIG. **5** in more detail. The process **207** is entered from the step **206** in FIG. **5**, after which a step **401** stores the biometric signature received by the step **203** in the memory **124** at a memory address defined by the card data **604** received in the step **202** of FIG. **5**. The aforementioned step **401** can store the biometric signature in encrypted form to reduce the probability that the signature can be acquired for unauthorised use, thus helping ensure the privacy of the card owner. The following steps **402** and **403** have the same respective functions as the corresponding steps **301** and **302** in FIG. **6**. After completion of the step **403**, the process **207** is directed back to the step **201** in FIG. **5**.

FIG. **8** shows the step **202** in FIG. **5** that is concerned with the processing of the card information **605** from the card **601** when the card **601** is read by the card reader **112** in the step **202** of FIG. **5**. The process **202** is entered from the step **201** in FIG. **5**, after which a step **501** reads the card information **605** from the card **601** using the card reader **112**. In a following step **502**, the processor **105** retrieves predefined "permitted card set" parameters to determine the "permitted card set" for the verification station **127** in question. A separate, or overlapping, permitted card set is defined for each verification station **127**. This ensures that a limited population of cards such as **601** undergo the BCP process at any given verification station **127**. This has the advantage of ensuring that the local memory **124** does not overflow, and it also provides control over which users make use of which verification stations.

In a following step **503** the processor **105** compares the header **606** against the predefined permitted card set parameters to determine if the card **601** belongs to the set of permitted cards for the verification station **127** in question. If this is the case, then the process **202** is directed by a YES arrow to the step **203** in FIG. **5**. If, on the other hand, the card header **606** does not belong to the permitted card set for the particular verification station **127**, then the step **202** follows a NO arrow from the step **503** to a step **504**. In the step **504**, the processor **105** rejects the card that has been entered into the card reader **112**. This rejection can take the form of a message displayed on the LCD display **126** and/or a corresponding audio message via the speaker **117**. Thereafter, the process **202** is directed back to the step **201** in FIG. **5**. It is noted that even if the verification station does not reject the card not belonging to the permitted card set for the verification station **127** in question, the back-end processor **122** can do so.

In addition to the predefined permitted card set, other administrative functions can be provided by the BCP arrangements. Thus, the predefined permitted card set details can be amended and/or the signatures stored in the database **124** can be deleted by a BCP system administrator. Audit trail information is also stored in the verification station **127** and can be downloaded for audit purposes. The audit information typically includes information of which cards have been submitted to the verification station and the time stamps of the card submissions. Biometric signatures are typically not part of the downloadable audit information, and require a greater level of authorisation (such as that associated with law enforcement agencies) for access.

FIG. **9** shows another application **900** to which the BCP arrangement can be applied. In a first step **901***a* person purchases or hires a verification station implemented in a portable form. A step **901** is performed at a registered supplier premises. Accordingly in a following step **902**, the enrolment process is performed in controlled circumstances at the supplier premises. The "controlled conditions" referred to mean that the enrolment process is performed under conditions where the identity of the holder of the card **601** is verified, using a driving licence, passport or equivalent identification document, this ensuring that the enrolment process enrols the true owner of the card in an authorised manner.

In a following step **903**, the verification station together with the card **601** can be used for third party transactions. Thus, in one example, the holder of the card **601** can take the

portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises. This station identification number is then transmitted to the on-line casino back-end processes together with the card information **605**. This type of application does require some modification of the back-end processes.

In another example, the holder of the card **601** takes the card **601** and the portable verification station **127** to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card **601** is able to apply the card to the card reader **112**, apply their biometric signature to the biometric reader **102**, and have the verification station **127** output the corresponding card information **605**. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card **601** is the authorised owner.

INDUSTRIAL APPLICABILITY

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP arrangements can, in general be used in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more.

Thus, for example, the BCP arrangement can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying platform.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is first issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room; negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to FIG. **5**.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim **1**;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

4. A method according to claim **3**, wherein the card device is one of:

a card in which the card information is encoded in a magnetic strip;

a card in which the card information is encoded in a bar code;

a smart card in which the card information is stored in a solid state memory on the smart card; and

a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

5. A method according to claim **3**, wherein:

the card information provided in the step (a) comprises a header and card data; and

the steps (c), (d) and (e) are only performed if the header indicates that the card belongs to a set of cards associated with the verification station.

6. A method according to claim **3**, wherein the performance of the process in the steps (db) and (eb) comprises outputting at least part of the inputted card information from the verification station.

7. A method according to claim **6**, wherein at least one of the steps (db) and (eb) comprise at least one of the further steps of:

inputting information from a keypad to the verification station; and

outputting at least some of the information input from the keypad.

8. A method according to claim **7**, wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

9. A method according to any one of claims claim **6**, **7** and **8** wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

10. A method according to claim **3**, wherein the step (ec) further comprises outputting information indicating that the user of the card device is not authorised authorized.

11. A method according to claim **10**, wherein the information outputted is communicated to one of:

a service provider for providing a service dependent upon receipt of the outputted information; and

an apparatus for providing access to a service dependent upon receipt of the outputted information.

12. A method according to claim **3**, comprising the further steps of:

(f) storing the card information provided by successive instances of the step (a); and

(g) outputting the information stored in the step (f) for audit purposes.

13. A biometric card pointer enrolment system comprising:

a card device reader for receiving card information;

a biometric reader for receiving the biometric signature;

means for defining, dependent upon the received card information, a memory location in a local memory external to the card;

means for determining if the defined memory location is unoccupied; and

means for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

14. A biometric card pointer verified access system comprising:

the biometric card pointer enrolment system of claim **13**; and

means for verifying (i) a subsequent presentation of card information to the card device reader and (ii) a subsequent presentation of a biometric signature to the biometric reader if said subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

15. A verification station for securing a process, the verification station comprising:

a card device reader for receiving card information from a card device coupled to the verification station;

a biometric signature reader for receiving a biometric signature provided to the verification station;

means for determining if the provided card information has been previously provided to the verification station;

means, if the provided card information has not been previously provided to the verification station, for:

storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

means, if the provided card information has been previously provided to the verification station, for:

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

16. A verification station according to claim **15**, wherein the card device reader is one of:

a reader for a card in which the card information is encoded in a magnetic strip;

a reader for a card in which the card information is encoded in a bar code;

a reader for a smart card in which the card information is stored in a solid state memory on the smart card; and

a receiver for a key fob adapted to provide the card information by transmitting a wireless signal to the verification station.

17. A verification station according to claim **15**, wherein the memory is incorporated in a tamper-proof manner in the verification station.

18. A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method for securing a process at a verification station, said program comprising:

code for determining if card information, provided to a card device reader incorporated into the verification station, has been previously provided to the verification station;

code, if the provided card information has not been previously provided to the verification station, for:

storing a biometric signature, inputted to a biometric signature reader incorporated into the verification station, in a memory incorporated into the verification station, at a memory location defined by the provided card information; and

performing the process dependent upon the received card information;

code, if the provided card information has been previously provided to the verification station, for:

comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

19. A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of enrolling in a biometric card pointer system, the program comprising:

code for receiving card information;

code for receiving the biometric signature;

code for defining, dependent upon the received card information, a memory location in a local memory external to the card;

code for determining if the defined memory location is unoccupied; and

code for storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

20. A non-transitory computer readable medium having recorded thereon a computer program for directing a processor to execute a method of obtaining verified access to a process, the program comprising:

code for storing a biometric signature according to the enrolment method of claim **19**;

code for subsequently presenting card information and a biometric signature; and

code for verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,620,039 B2
APPLICATION NO. : 12/063650
DATED : December 31, 2013
INVENTOR(S) : Christopher John Burke

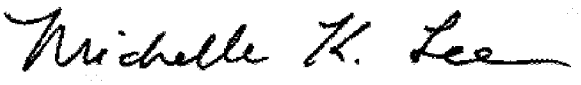
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page:

The first or sole Notice should read --

Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1707 days.

Signed and Sealed this
Twenty-second Day of September, 2015



Michelle K. Lee
Director of the United States Patent and Trademark Office

FORM 19. Certificate of Compliance with Type-Volume Limitations **Form 19**
July 2020

UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATIONS

Case Number: 24-1365

Short Case Caption: CPC Patent Technologies Pty Ltd. v. Apple Inc.

Instructions: When computing a word, line, or page count, you may exclude any items listed as exempted under Fed. R. App. P. 5(c), Fed. R. App. P. 21(d), Fed. R. App. P. 27(d)(2), Fed. R. App. P. 32(f), or Fed. Cir. R. 32(b)(2).

The foregoing filing complies with the relevant type-volume limitation of the Federal Rules of Appellate Procedure and Federal Circuit Rules because it meets one of the following:

☑ the filing has been prepared using a proportionally-spaced typeface and includes 4,229 words.

☐ the filing has been prepared using a monospaced typeface and includes _____ lines of text.

☐ the filing contains _____ pages / _____ words / _____ lines of text, which does not exceed the maximum authorized by this court's order (ECF No. _____).

Date: 04/29/2024

Signature: /s/ George Summerfield

Name: George Summerfield

Save for Filing